DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN, PARA EL ÁREA DE TI, DE LA COMPAÑÍA INDUCON UBICADA EN LA CIUDAD DE BOGOTÁ

ANA CECILIA CASTRILLÓN BARRETO
JUAN PABLO FALLA SÁNCHEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN, PARA EL ÁREA DE TI, DE LA COMPAÑÍA INDUCON UBICADA EN LA CIUDAD DE BOGOTÁ

ANA CECILIA CASTRILLÓN BARRETO
JUAN PABLO FALLA SÁNCHEZ

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

Asesor
Ing. Juan Carlos Alarcón

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

Nota de Aceptación

_____

_____

_____

_____
Firma presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C., mayo de 2015

A nuestros padres, familiares y esposo(a) porque nos brindaron su apoyo moral para seguir estudiando y lograr el objetivo trazado para un mejor futuro y ser un orgullo para ellos y toda la familia.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A la Universidad Piloto de Colombia

A todas aquellas personas que de una u otra manera han colaborado en la elaboración de este proyecto.

A las directivas de INDUCON por permitir realizar este plan de trabajo, y a todo el grupo de trabajo por su valiosa participación.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

BCP: “es un método de análisis, definición y diseño de la arquitectura de la información de las organizaciones”[1].

CAD: “diseño asistido por computador”[2].

CAM: “fabricación asistida por computador”[3].

CONFIDENCIALIDAD: la información solo la vean los que estén autorizados.

DISPONIBILIDAD: la información esté disponible.

DOFA: herramienta administrativa que permite realizar diagnóstico de una empresa compuesta por matriz con (Debilidades, Oportunidades, Fortalezas y Amenazas).

INTEGRIDAD: la información mantenga su completitud sobre todo su ciclo de vida

ISO: “organización internación de estandarización”[4].

SGSI: “sistema de gestión de seguridad de la información”[5].

TI: tecnología de información

TIC: tecnología de la información y comunicaciones

[1] DINERO E IMAGEN. La importancia de implementar un plan de continuidad de negocio [en línea]. Bogotá: La Empresa [citado 1 julio, 2013]. Disponible en Internet: <URL: http://www.dineroenimagen.com/2013-07-01/22403>

[2] WIKIPEDIA. Diseño asistido por computadora [en línea]. Bogotá: Wikipedia [citado 23 enero, 2015]. Disponible en Internet: <URL: https://es.wikipedia.org/wiki/CAD/CAM>.

[3] WIKIPEDIA. Fabricación asistida por computadora [en línea]. Bogotá: Wikipedia [citado 23 enero, 2015]. Disponible en Internet: https://es.wikipedia.org/wiki/CAD/CAM>

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO. ISO International Standards [en línea]. Ginebra: ISO [citado 23 enero, 2015]. Disponible en Internet: <http://www.iso.org/iso/home/standards.htm>

[5] EL PORTAL DE ISO 27001 EN ESPAÑOL. ISO 27000 SGSI Sistema de Gestión de Seguridad de la Información [en línea]. Bogotá: El Portal [citado 23 enero, 2015]. Disponible en Internet: <URL: http://www.iso27000.es/sgsi.html>.

INTRODUCCIÓN

En la época de la sociedad del conocimiento en la que se desarrolla el mundo actual, se hace necesario que las empresas dediquen esfuerzo, tiempo y recursos para la protección del activo más valioso como es la información; es por esta razón que al revisar el tema de gobierno de TI en la empresa INDUCON de Colombia se evidencia la necesidad de realizar el diseño de un plan de seguridad de la información, para el área de TI de la compañía, cuyo objetivo de negocio es el diseño, corte y confección de dotaciones industriales y prendas militares a nivel nacional e internacional.

Una vez terminado el trabajo de investigación aplicada se suministrará a INDUCON el diseño de un plan de seguridad de la información, para los procesos críticos del área de TI, mapa de riesgos, concientizar, capacitar y lograr en conjunto con la alta gerencia de INDUCON la definición y aprobación de una política de seguridad de la información, con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información.

Para la realización de los objetivos anteriores se contó con un tiempo de 5 meses, tiempo en el cual se realizó el levantamiento de información, identificación y definición procesos de TI para el desarrollo del mapa de riesgos de estos, diseño del plan de tratamiento de riegos y la implementación de algunos controles. Todos los anteriores elementos conforman lo que se denominó EL “PLAN DE SEGURIDAD DE LA INFORMACIÓN, PARA EL ÁREA DE TI DE INDUCON”.

1. FORMULACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

La empresa INDUCON está ubicada en la ciudad de Bogotá, es una Sociedad por Acciones Simplificada, con 30 años de trayectoria en la confección de dotaciones industriales con la mejor calidad, está especializada en confección de ropa y accesorios para protección personal, identificación corporativa, uniformes y prendas militares. Cuenta con lo último en tecnología de corte CAM (fabricación asistida por computador). La información obtenida de diseño y patronaje es interpretada por técnicos expertos en el manejo de esta maquinaria, apoyados por profesionales del diseño de modas y dotados de sistemas CAD (Diseño Asistido por Computador), cuenta con una aplicación centralizada SAP *BUSINESS ONE* para la administración de todos sus procesos, aplicaciones de ingeniería STYM para el control de métodos y tiempos, con la ayuda del aplicativo *Willcom* para el diseño de bordados, con toda esta tecnología INDUCON busca brindar la mejor calidad en la producción y confección satisfaciendo así a todos sus clientes.

A pesar que cuenta con estos recursos tecnológicos, presenta algunos problemas entre los que se enmarcan la no existencia de procedimientos, de políticas de uso de recursos de TI, un manejo detallado de inventarios y control de máquinas, no cuentan con un mapa de análisis de riesgos, un plan de continuidad de negocio (BCP), una definición de roles y responsabilidades por función tecnológica, un sistema que ayude a la gestión de incidentes de seguridad de la información, INDUCON no cuenta con un plan de seguridad de la información para el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información que le permita asegurar la confidencialidad, integridad y disponibilidad de los activos de información que minimice a la vez los riesgos inherentes al uso de tecnología. En relación a los problemas y deficiencias encontradas, se priorizará en definir un plan de seguridad de la información para el área de TI.

El problema inicial estaría enfocado a resolver la pregunta ¿Cómo diseñar un plan de seguridad de la información, para el área de TI en la empresa INDUCON que le proporcione una herramienta para gestionar los procesos de tecnología y reducir los riesgos de seguridad de la información?.

1.2 JUSTIFICACIÓN

La seguridad informática es el área de la informática que: “Se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (se centra básicamente en hardware y software) y que éstas sean utilizadas de la manera indicada por la organización. Su análisis de riesgos

se centra en vulnerabilidades del hardware o software y llevar el nivel de riesgo a nivel aceptable por la organización"[6].

La seguridad informática se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y normas concebidas para minimizar los posibles riesgos a la infraestructura o a la información, los cuales propenden por la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Este proyecto busca diseñar un plan de seguridad de la información para el área de TI que proporcionará a la compañía INDUCON mejora en el flujo de los procesos de TI, que apoyan los procesos misionales de la compañía. Con el levantamiento del mapa de riesgos se contará con una herramienta de gestión administrativa para gestionar las amenazas y vulnerabilidades del área de TI, mediante el diseño de políticas procedimientos y controles específicos, adicionalmente, se verá reflejada una disminución de costos de acuerdo a un manejo eficiente de los recursos y las inversiones innecesarias, para la preservación de la seguridad de TI, es importante resaltar que el diseño de un plan de seguridad de la información para el área de TI ayudará a cumplir con la legislación vigente, reduciendo la posibilidad de incurrir en sanciones que afecten a la compañía, su imagen corporativa y clientes.

Debido a la complejidad de los procesos de INDUCON y restricciones de tiempo para la realización del proyecto, el diseño del plan de seguridad de la información se realizó para el área de TI y en específico para las actividades que intervienen y soportan los sistemas de información críticos: ERP SAP *Business One* y las actividades de acceso a los recursos de los servidores, aplicaciones y bases de datos, perfiles de usuarios, seguridad perimetral, igualmente, protección y seguridad a la infraestructura tecnológica sobre la cual funcionan éstas, como son el centro de datos y la infraestructura de red.

1.3 OBJETIVOS

1.3.1 Objetivo General. Diseñar un plan de seguridad de la información para el área de TI en la empresa INDUCON ubicada en la ciudad de Bogotá, mediante la realización de un diagnóstico para determinar las brechas de seguridad, levantamiento del mapa de riesgos de los procesos de TI y la definición de la política general de gobierno de seguridad de la información, con el fin de suministrar a INDUCON en un término de cinco meses el documento del plan de seguridad de la información.

[6]CAMELO, Leonardo. Marco legal de Seguridad de la información [en línea]. Seguridad en Información en Colombia [citado 18 febrero, 2010]. Disponible en Internet: <URL: http://seguridadinformacion Colombia. blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html>.

1.3.2 Objetivos Específicos

- Realizar un diagnóstico para determinar brechas de seguridad informática en el área de TI alineados a los objetivos del negocio de la compañía INDUCON.

- Realizar un mapa de riesgos para el área de TI para la compañía INDUCON.

- Concientizar a las directivas de la compañía INDUCON de la importancia de definir una política general de gobierno de seguridad de la información.

2. MARCO TEÓRICO

2.1 TEORÍA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un Sistema de gestión de seguridad de la información –SGSI, comprende la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la información. De este modo un SGSI se implanta de acuerdo a estándares de seguridad como el ISO 27001, el cual se basa en códigos de buenas prácticas y objetivos de control como los establecidos en la ISO 27002.

La implantación de un SGSI se centra en la preservación de las características de confidencialidad, integridad y disponibilidad, mediante la aplicación de un proceso de gestión del riesgo. Por lo anterior, resulta imprescindible que las entidades identifiquen los riesgos que pueden afectar su información y sus activos, de manera que se pueda crear un plan para tratar apropiadamente los riesgos.

Como lo define la norma ISO 27001, "la adopción de un SGSI es una decisión estratégica para la organización y el establecimiento e implementación del SGSI tienen influencia en las necesidades y objetivos de ésta, los requisitos de seguridad, los procesos organizacionales empleados, el tamaño y estructura de la organización"[7]. El establecimiento del SGSI incluye definir cuál será el alcance, límites y por tanto la política de seguridad de la información, para luego implementar y operar el SGSI, diseñar y ejecutar procedimientos de seguimiento, revisión y otros controles que permitan definir después cuáles serán las acciones de mantenimiento y mejora.

2.2 CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO

2.2.1 Contexto Interno. Industrias y Confecciones INDUCON SAS, es una empresa del sector de fabricación, dedicada a la confección de dotaciones industriales con la mejor calidad, especializada en confección de ropa y accesorios para protección personal, identificación corporativa uniformes y prendas militares. Entre sus clientes se encuentran: Alpina, Carrefour, Avianca, Pavco, Zenú, Meals de Colombia S.A., Ministerio de Minas y Energía, Ministerio de Defensa Nacional entre otros.

INDUCON, nace en abril 28 de 1984, como el desarrollo de una idea de negocio de su fundador. Como todo lo que se construye con esfuerzo y dedicación, INDUCON ha logrado tomar forma y abrirse un espacio importante dentro del

[7] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001. Bogotá: ICONTEC, 2013. p. 7.

gremio de las confecciones, ubicándose como una de las empresas de mayor reconocimiento en el campo de las dotaciones industriales y prendas militares a nivel nacional e internacional, incorporando a su infraestructura la mejor mano de obra, y lo último en CAD (tecnología de diseño asistido por computador), corte y confección, actualmente cuenta con aproximadamente 250 trabajadores, dentro de los cuales se destacan profesionales en diseño de modas, técnicos expertos en el manejo de tecnología de corte CAM (fabricación asistida por computador), personal experto y calificado en corte y confección, expertos en control de calidad, operarios entre otros.

Para INDUCON un uniforme es una prenda que traduce una imagen adecuada, es la apariencia visible de una persona o profesión, lo que se proyecta a la sociedad y esta a su vez percibe de quien la viste, un uniforme traduce el compromiso, el amor y la identidad profesional, proyecta la capacidad de impartir justicia, dar y recibir respeto, asumir responsabilidad, brindar comprensión, esperanza, tolerancia y prudencia.

A continuación se transcriben los elementos fundamentales de la plataforma estratégica de INDUCON

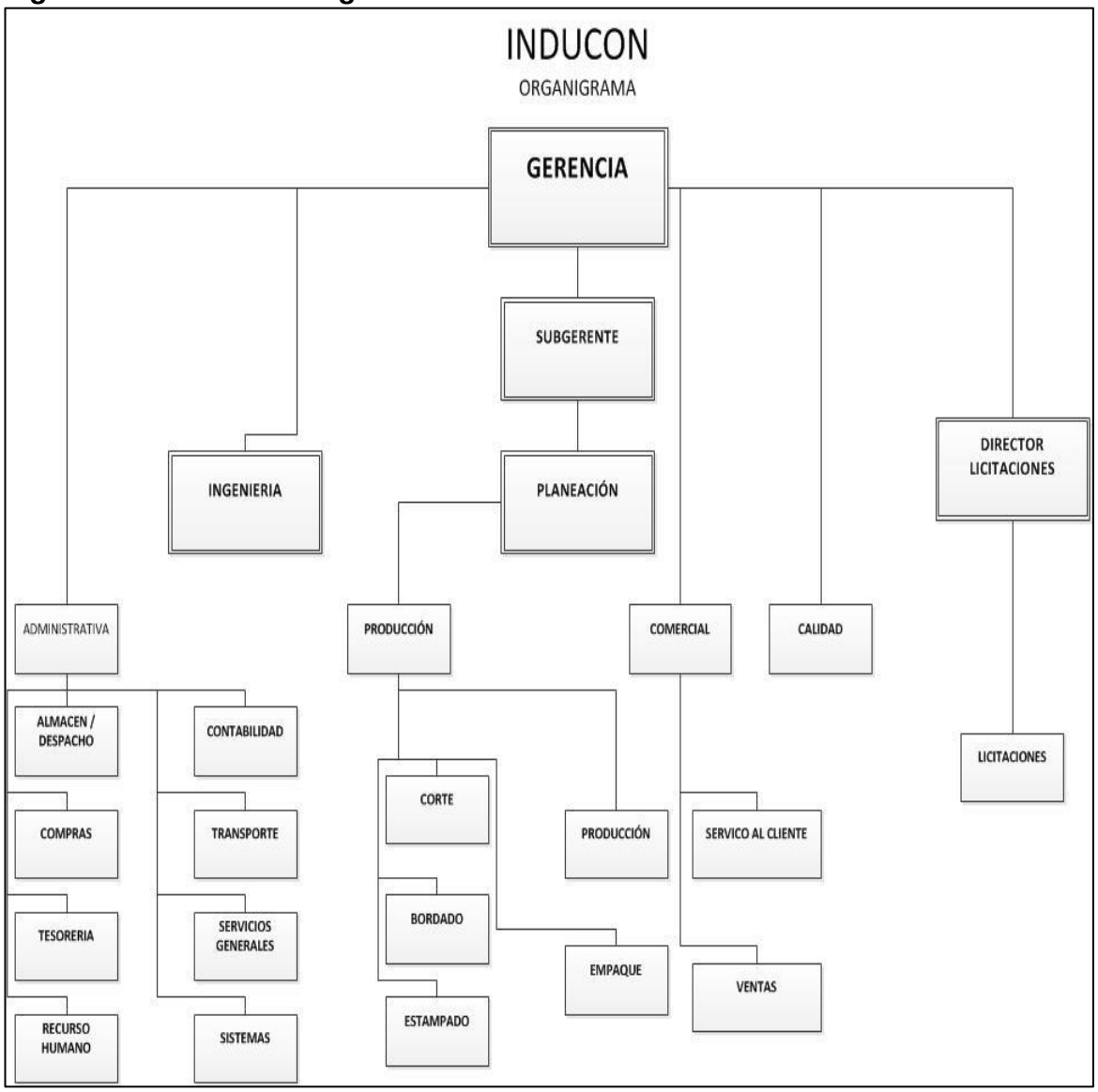
➢**Valores.** La gente que conforma nuestra empresa tiene definida la misión de participar activamente en la elaboración de prendas de vestir casual, uniformes y ropa para trabajo que brinden al usuario el máximo de confort, calidad, distinción e identificación corporativa.

➢**Objetivos.** Con nuestra experiencia y el continuo mejoramiento, queremos ser líderes en confección de uniformes, logrando permanecer en el mercado y conseguir la preferencia y fidelidad de cada uno de nuestros clientes y usuarios.

➢**Eslogan.** En INDUCON creamos prendas que traducen el verdadero propósito de quien las viste.

➢**Estructura Orgánica.** A continuación se ilustra las diferentes áreas que componen la empresa INDUCON (véase la Figura 1).

Figura 1. Estructura Orgánica de INDUCON



Fuente. Los Autores.

2.2.1.1 Descripción de las Funciones Principales del Departamento de TI. El objetivo del área de tecnología de INDUCON, es mantener la disponibilidad de las tecnologías de información y soportar las demás áreas que hacen parte de la compañía, brindando soporte 7*24. Actualmente la planta de personal del área de TI se apoya en un Ingeniero de Sistemas, quien cumple con las siguientes funciones:

A continuación se especifican las diferentes actividades o funciones que desempeña el Ingeniero de Sistemas actualmente en la compañía INDUCON (véase el Cuadro 1).

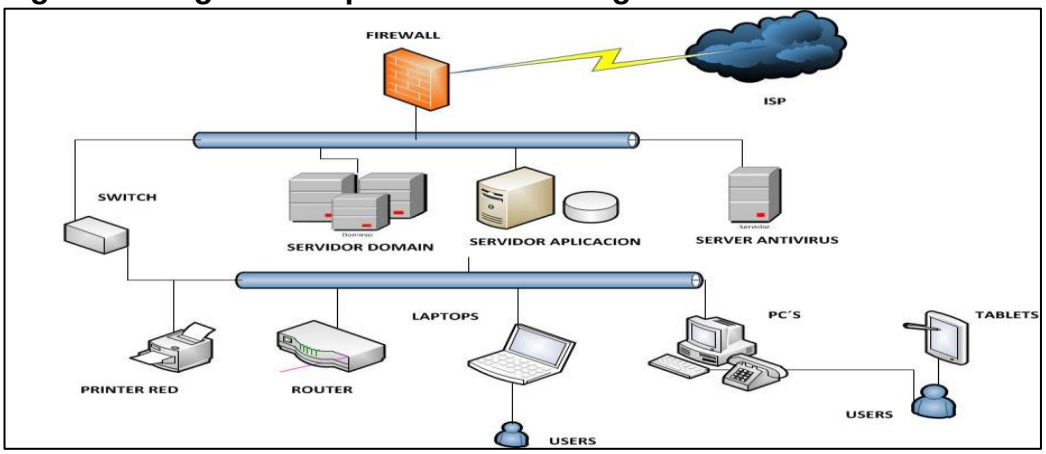
Cuadro 1. Descripción de Funciones

Ingeniero de Sistemas	Objetivo: Coordinar las actividades referentes a TI, brindar soporte a nivel de aplicación y gestión, garantizar el buen funcionamiento del hardware, software y demás recursos tecnológicos que apoyan la gestión de INDUCON como son las redes de comunicación y servidores.
Responsabilidad	
➢Mantenimiento de computadores software y hardware. ➢Soporte aplicaciones ofimáticas y de escritorio. ➢Soporte de aplicación SAP Business One nivel 1 y 2. ➢Administración base de datos en SQL Server 2008 donde se aloja la información del aplicativo SAP, Gestión de backups y procedimientos. ➢Gestionar los diferentes reportes que solicitan las áreas desarrollados en CrystalReport. ➢Administración de servidor de directorio activo en sistema operativo Windows 2008 server estándar R2 ➢Administración servidor de aplicación SAP BO en plataforma Windows 2008 server R2 estándar. ➢Administración de la plataforma de correos. ➢Cumplimiento de la adquisición de software legal. ➢Administración y control de software de terceros donde se encuentran Helisa SGW software contable, Diamino y Modaris aplicativos para el diseño de prendas, Stym aplicativo de métodos y tiempos, plataforma de relojes biométricos, cámaras de seguridad y alarma. ➢Administración de la seguridad perimetral, donde se cuenta con un Firewall Sonicwall, consola administrativa de Kaspersky donde se maneja toda la parte centralizada de los equipos. ➢Administración y control de las comunicaciones con las que cuenta la compañía como son servicio de Internet y plataformas internas de comunicación inalámbrica routers. ➢Administración de la arquitectura física de red. ➢Administración de compra de nuevas tecnologías que cumplan las condiciones específicas y técnicas para nuevos requerimientos. ➢Administración y control herramienta colaborativa web utilizada para agendar las actividades de los usuarios administrativos de INDUCON.	

Fuente. Los Autores.

En la Figura 2 se ilustran los diferentes componentes de red y dispositivos de conexión para la comunicación interna y externa de la compañía.

Figura 2. Diagrama Arquitectura tecnológica INDUCON



Fuente. Los Autores.

➢**Nivel de conocimiento.** Actualmente la compañía cuenta con un Ingeniero de sistemas con experiencia y conocimiento, apoyado en la capacitación constante en temas de tecnología y administración, buscando fortalecer las necesidades que tiene actualmente INDUCON, apoyados con los diferentes entidades prestadoras de servicios.

➢**Infraestructura Tecnológica de INDUCON.** Los componentes tecnológicos sobre la cual soporta los procesos de tecnología INDUCON se pueden resumir en:

✓Aplicación SAP, ERP que normaliza todos los procesos integrados en una sola herramienta.

✓Software Modaris y Diamino, para diseño y corte de las prendas.

✓Software Willcom para bordados.

✓Tecnología de alto nivel para apoyar los procesos de corte con una máquina automática, todos estos apoyados en una arquitectura de red basada en servidores de aplicación, base de datos y dominio para centralizar la administración de la red en un solo punto y controlar el acceso a los usuarios.

✓Equipos activos de red que permiten la comunicación con toda la infraestructura tecnológica.

✓Dispositivos de entrada y salida como son impresoras de gran formato, de formato estándar y plotters.

✓Estaciones de trabajo para el desarrollo de las actividades y tareas por parte de los empleados, quienes utilizan herramientas de ofimática, correo electrónico para la comunicación interna y externa.

✓Las aplicaciones que soportan el core del negocio están debidamente licenciadas y con contratos de mantenimiento y soporte.

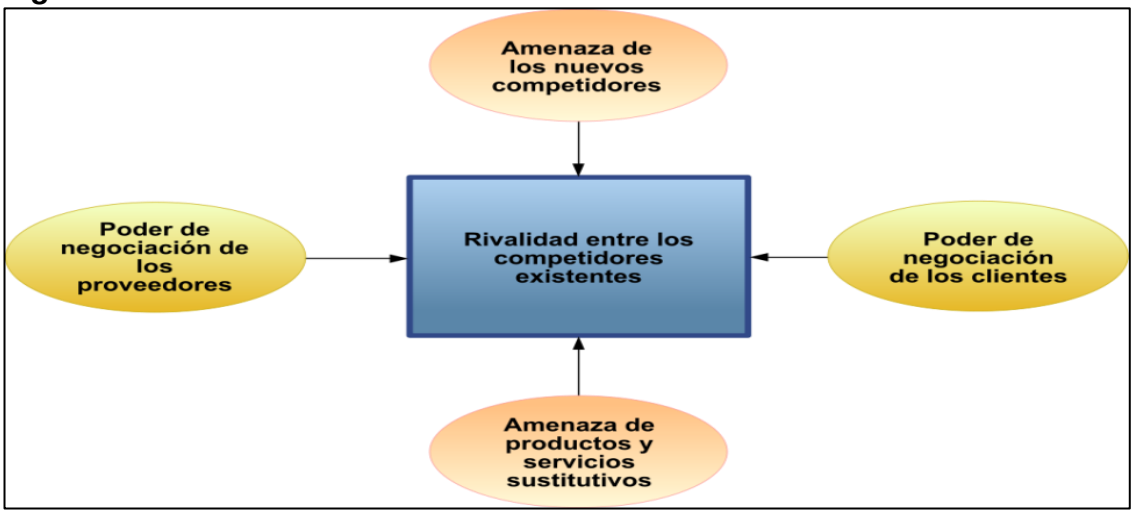
2.2.2 Contexto Externo. Confecciones INDUCON, es consciente que el proceso de globalización es imposible de ignorar y que por lo tanto, debe aplicar estrategias para estar a la vanguardia en el sector de la confección. La empresa está decidida a implementar un proceso de mejoramiento continuo, encaminado a la búsqueda del control de los procesos, definición de políticas de calidad y de seguridad de la información y definir determinados planes como el de este proyecto.

Igualmente, INDUCON tiene presente el modelo de análisis de la competencia de las cinco fuerzas de Michael Porter (véase la Figura 3), el cual es utilizado por muchas industrias como instrumento de gestión para la elaboración de estrategias tomando en cuenta el entorno externo.

Tomando como base el modelo de Porter, se realizó con el área de mercadeo un análisis estratégico haciendo referencia a la posición actual de la compañía y su entorno competitivo internacional, se validó el ambiente nacional, el cual busca determinar el contexto donde opera la compañía, sus ventajas competitivas en el mercado mundial y un factor importante, es la parte legal y tecnológica, que pueden en un momento dado afectar la organización.

Una de las amenazas que enfrenta INDUCON, es la competencia, se sabe que entre mayor competencia, menor fuerza y por consiguiente el riesgo es más alto y las utilidades también se reducen de una manera proporcional.

Figura 3. Modelo de las Cinco Fuerzas de PORTER



Fuente. PORTER, Michael E. Modelo de las cinco fuerzas de Porter [en línea]. Bogotá: Wikipedia [citado 18 febrero, 2015]. Disponible en Internet: <URL: es.wikipedia.org/wiki/Análisis_ Porter_de_las_cinco_fuerzas>.

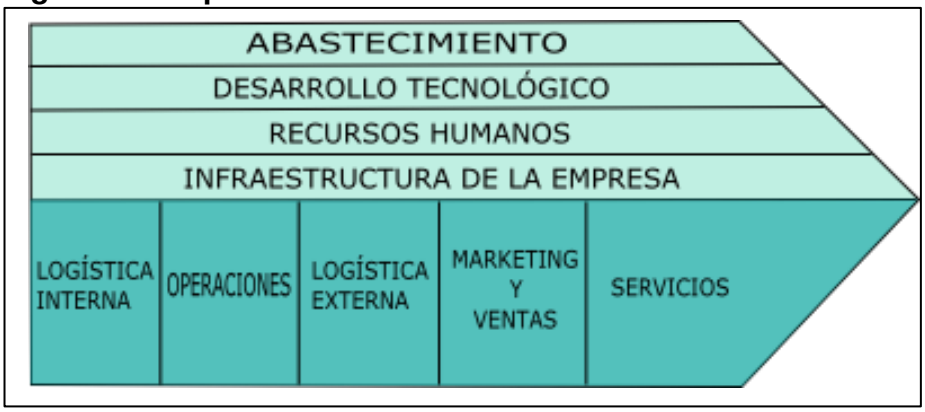
Igualmente, se evidencia una amenaza que a la vez puede ser una fortaleza para INDUCON, es la rivalidad entre las empresas que actualmente son competencia en la producción de prendas industriales y militares, los cambios son más rápidos, y la competencia en el precio, es sin duda una de las partes que más afecta en la fabricación y comercialización de las prendas industriales, la fortaleza de INDUCON frente a esta competencia es la trayectoria y el reconocimiento en el mercado nacional e internacional en la calidad de elaboración de sus prendas.

En contexto con lo anterior, en INDUCON se tiene establecido personal idóneo para realizar las actividades y procesos, que generan un fortalecimiento en la entrega final del producto apoyados en la tecnología e infraestructura; buscando siempre ofrecer una calidad de servicio a los clientes.

Con respecto a las etapas de producción se busca siempre las rutas críticas o caminos más cortos, para la elaboración del producto, apoyados con aplicaciones que ayudan a validar los métodos y tiempos, como es la herramienta STYM.

En INDUCON, también para el análisis tanto del contexto interno como externo, se tiene en cuenta la cadena de valor empresarial o cadena de valor de Michael Porter (véase la Figura 4), que es un modelo teórico que permite describir el desarrollo de las actividades de una organización empresarial, generando valor al cliente final, INDUCON a nivel nacional cuenta con grandes marcas o superficies y se tienen algunos clientes internacionales, todos ellos con expectativas de mejoras en el mercado.

Figura 4. Esquema de la cadena de valor de Porter



Fuente. PORTER, Michael E. Modelo de las cinco fuerzas de Porter [en línea]. Bogotá: Wikipedia [citado 18 febrero, 2015]. Disponible en Internet: <URL: es.wikipedia.org/wiki/Análisis_ Porter_de_las_cinco_fuerzas>.

Las entidades reguladoras y de control que supervisan a INDUCON son la DIAN, que valida el cumplimiento de las obligaciones tributarias, impuestos y demás, entidades como el VUCE Ventanilla Única de Comercio Exterior encargada de

adelantar los trámites de comercio exterior ante 21 entidades del estado, a través de un solo canal, que garantiza la seguridad tecnológica y jurídica de los diferentes trámites, integrando la firma digital.

INDUCON cuenta con algunos socios estratégicos, que le permiten cumplir con algunas condiciones contractuales para las licitaciones públicas con entidades como la Fuerza Aérea, Ejército Nacional, la Armada Nacional que exigen un capital financiero muy alto.

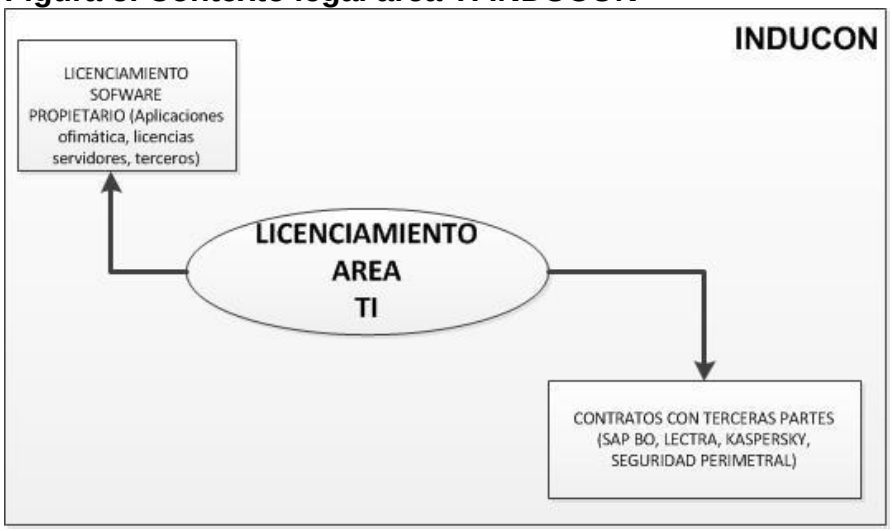
Respecto a factores tecnológicos INDUCON, cuenta con infraestructura tecnológica, maquinaria y equipos, que soportan los procesos que se llevan a cabo día a día, busca permanentemente estar actualizados con nuevas tecnologías, que permitan brindar mayor rendimiento y efectividad en el momento de la elaboración de las prendas o dotaciones, buscando siempre automatizar aquellos procesos manuales, dando garantía en el cumplimiento de plazos de entrega hacia los clientes y beneficiando a los colaboradores en sus tiempos.

2.2.3 Contexto Legal. INDUCON cuenta con varios proveedores de servicios, con quienes realiza contratos de licenciamiento de uso y mantenimiento de software; tanto para servidores como para los equipos cliente, como son: para la aplicación SAP BO Software, que cumple el papel de ERP para las funciones de la compañía, así como para los aplicativos de diseño y corte de las prendas como son: Willcom, Lectra, Modaris e incluyendo la suite de Corel Draw, licenciamiento del Sistema Operativo y Base de datos.

Igualmente, para la contratación se rige bajo las normas del código de comercio, ley 80 de 1993 – estatuto general de contratación, ley 1150 de 2007, decreto 2474 - de contratación, ley 527 de 1999 – se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, decreto 1747 de 2000 – se reglamenta parcialmente la ley 527/99 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

A continuación se ilustra el contexto legal de INDUCON, evidenciando las partes interesadas que conforman el licenciamiento y contratos que tiene vigente la compañía (véase en la Figura 5).

Figura 5. Contexto legal área TI INDUCON



Fuente. Los Autores.

2.2.4 Secreto Industrial o comercial. INDUCON, se acoge al artículo 260 de la decisión 486 de 2000 de la Comisión de la Comunidad Andina, el cual estipula que:

Se considerará como secreto empresarial cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida que dicha información sea:

- Secreta, en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes, no sea generalmente conocida ni fácilmente accesible, por quienes se encuentran en los círculos, que normalmente manejan la información respectiva;

- Tenga un valor comercial por ser secreta;

- Haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta.

"La información de un secreto empresarial podrá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios"[8].

[8] COMUNIDAD ANDINA. Decisión 486 de 2000 - Régimen Común sobre Propiedad Industrial [en línea]. Lima: La Comunidad [citado 18 febrero, 2015]. Disponible en Internet: <URL: www.comunidadandina. org/Sección.aspx?id...propiedad-intelectual>.

2.2.5 Matriz DOFA. Una vez realizado el contexto interno y externo, se procede a definir la matriz DOFA, ver cuadro 2, el cual hace referencia a las debilidades, oportunidades, fortalezas y amenazas; con el fin de suministrar a las directivas de INDUCON, una herramienta para el desempeño; tanto presente como futuro de la compañía; la cual puede ser completada de acuerdo a las perspectivas de sus directivos (véase el Cuadro 2).

Cuadro 2. Matriz DOFA

Fortalezas	**Debilidades**
➢Infraestructura tecnológica de TI y sistemas de información actualizados para el desarrollo del diseño y confección de las prendas. ➢Infraestructura física le permite tener espacios adecuados para el desarrollo de su función. ➢Adecuado desarrollo de la salud ocupacional y condiciones físicas para el trabajador. ➢Talento humano calificado y comprometido.	➢No existe un Sistema de Gestión de Calidad. ➢Falta definición y fijación de políticas de seguridad de la información, modelos de gestión enfocada en procesos. ➢No hay definición de manual de funciones por competencias y definición de roles y responsabilidades. ➢Deficiencia de procedimientos para la gestión adecuada de TI.
Oportunidades	**Amenazas**
➢Tendencia al crecimiento. ➢Establecer alianzas estratégicas con entidades del sector. ➢Implementar el Sistema de Gestión de Calidad. ➢Implementar el SGSI a mediano plazo. .	➢Rivalidad entre competidores, competencia desleal. ➢ Precios bajos de la competencia. ➢Debe conocer un poco más a sus competidores. ➢La competencia sonsaca a empleados de la compañía.

Fuente. Los Autores.

Es de anotar, que la matriz DOFA está centrada en el tema de seguridad de la información. A continuación se presenta la matriz y el análisis respectivo.

2.2.5.1 Análisis DOFA. A continuación se realiza el análisis DOFA, (véase el Cuadro 3), en el cual, se realiza formulación de estrategias y alternativas de acuerdo a sus fortalezas- oportunidades, a sus debilidades - oportunidades, a las fortalezas - amenazas y a las debilidades y amenazas de INDUCON.

Cuadro 3. Análisis DOFA

No.	Fortalezas - Oportunidades	No.	Debilidades - Oportunidades	No.	Fortalezas -Amenazas	No.	Debilidades – Amenazas
FO1	Fortalecer la infraestructura de TI y los sistemas de información de diseño y confección de las prendas, para fortalecer el crecimiento en el mercado.	DO1	Implementar un sistema de gestión de calidad, que aporte para su desarrollo y crecimiento.	FA1	Aprovechar la infraestructura tecnología y sus sistemas de información para realizar inteligencia de negocios para generar estrategias de fidelización de clientes entre otras.	DA1	Implementar sistemas de gestión para fortalecer sus procesos, lo que le dará un plus ante sus competidores.
FO2	No aplica	DO2	Definir y formalizar políticas de seguridad de la información y modelos de gestión enfocada a procesos para realizar alianzas estratégicas con entidades del sector.	FA2	Realizar negociaciones con los proveedores, de acuerdo a la demanda de los productos a precios razonables, aprovechando los espacios disponibles para el almacenaje de los insumos.	DA2	Definir políticas de seguridad de la información y modelos de gestión enfocada en procesos, contribuirá a minimizar tiempos optimizar las operaciones de la entidad y los recursos, permitiendo realizar estudios de costos, revisar los precios de los artículos y generar valor agregado de servicio al cliente.
FO3	Empoderar y aprovechar el adecuado desarrollo de la salud ocupacional y las condiciones físicas del trabajador, para obtener sus aportes y sugerencia en el estudio inicial para implementar el sistema de gestión de calidad.	DO3	Implementar el manual de funciones por competencias y definir roles y responsabilidades le proporciona a la entidad herramientas claves para la implementación del SGSI.	FA3	Realizar estudio para establecer debidamente el contexto externo de la entidad, con énfasis en definición de un modelo de estrategias competitivas del sector de la confección.	DA3	Definir manual de funciones y roles, dotará a la entidad de una herramienta y podrá definir roles para realizar estudios de mercado, que permitirán conocer un poco más a la competencia.
FO4	Empoderar y generar sinergia en el talento humano, enfocándose en la necesidad y los beneficios de implementar un SGSI.	DO4	Implementar un modelo de gestión por procesos redundará en grandes avances para la implementación del SGSI.	FA4	Generar políticas de gestión del talento humano, de incentivos y reconocimiento contribuirá a que el talento humano logre los objetivos planteados y le aporte para su proyecto de vida y compromiso y fidelidad a la compañía.	DA4	Establecer un modelo de gestión enfocado en procesos, reduce el desgaste administrativo y del talento humano por reproceso en sus actividades, generando menos estrés de las personas y mayor compromiso.

Fuente. Los Autores.

2.3 ANÁLISIS DEL CONTEXTO

INDUCON es una empresa que pertenece al sector de las confecciones, su plataforma estratégica está definida de acuerdo a su objetivo de negocio, posee una infraestructura física y tecnológica que responde a sus necesidades, cuenta con sistemas de información y aplicaciones que soportan el core del negocio, apoyan la misión y la visión de la entidad. Su recurso humano está capacitado y es idóneo para cumplir con los objetivos de negocio, pero se evidencia deficiencia de personal en el área de TI, su estructura orgánica es jerárquica pero no existe un organigrama definido, por lo que se realizó levantamiento del mismo durante el desarrollo del trabajo de investigación.

Las directivas de la empresa son conscientes que sus competidores son fuertes y que la forma de mantenerse en el mercado es generando productos con calidad y oportunidad para sus clientes. A continuación se realiza el análisis del contexto externo utilizando el modelo de las cinco fuerzas de Porter y el análisis de contexto interno utilizando el modelo de la cadena de valor de Michael Porter para INDUCON.

2.3.1 Modelo de las Cinco Fuerzas de Porter para INDUCON.

2.3.1.1 Rivalidad entre Competidores.

- Competencia desleal aunque estamos en el mismo mercado mismo idioma las empresas ofrecen los productos más baratos, con el fin de sacar a las otras empresas del mercado.

- Existe una disminución considerada en el precio.

- INDUCON es considerada para los otros competidores como una empresa competitiva y grande en el mercado cuando se refiere a contrataciones estatales.

- Identificación de los competidores. Delmyp es una empresa bastante grande en infraestructura y maneja otros productos que INDUCON actualmente no ofrece, empresas como Inboutex y Texman, están en el mismo grado de capacidad, los demás competidores son de tamaño desigual.

- Grado de diferenciación. INDUCON y Delmyp están a la vanguardia en tecnología, diferenciándose por la antigüedad en el mercado, por la calidad de las prendas y en los tiempos de entrega.

2.3.1.2 Amenaza de los Nuevos Competidores. La amenaza de nuevos competidores a nivel local, es considerada como una amenaza catalogada como media, esto a raíz de que los competidores no muy grandes requieren de una capacidad financiera bastante alta y una capacidad de producción para soportar

niveles altos de confección. Actualmente INDUCON realiza campañas publicitarias y de marketing, con la finalidad de realizar distribución oportuna de los productos a sus clientes y fidelizarlos, ofrece servicios a pequeños satélites con el fin de garantizar su distribución, en el mercado internacional existen varias restricciones a nivel estatal para la confección, ya que exigen que el producto sea nacional.

La necesidad de obtener tecnología y conocimiento especializado es otro factor importante para los competidores de menor escala, la falta de experiencia en el mercado, falta de canales adecuados para la distribución, falta de acceso a materias primas, son factores que obligan a que los competidores se fortalezcan en estas áreas en la que INDUCON es fuerte.

2.3.1.3 Amenaza de Productos y Servicios Sustitutos. Existen una variedad de productos sustitutos que INDUCON no produce, porque es más rentable subcontratar con el proveedor que se dedica a esa línea de productos.

Como los mayores clientes son entidades estatales y gubernamentales las especificaciones de los productos deben cumplir con requerimientos técnicos y normativos, lo cual no permite el manejo de productos sustitutos en esta línea de confección.

2.3.1.4 Poder de Negociación de los Proveedores. La mayoría de productos que requieren de telas específicas no son de fácil cambio por su costo y no son producidas por muchos proveedores, por lo tanto, no es fácil cambiar de proveedor de un momento a otro porque afecta la producción**.**

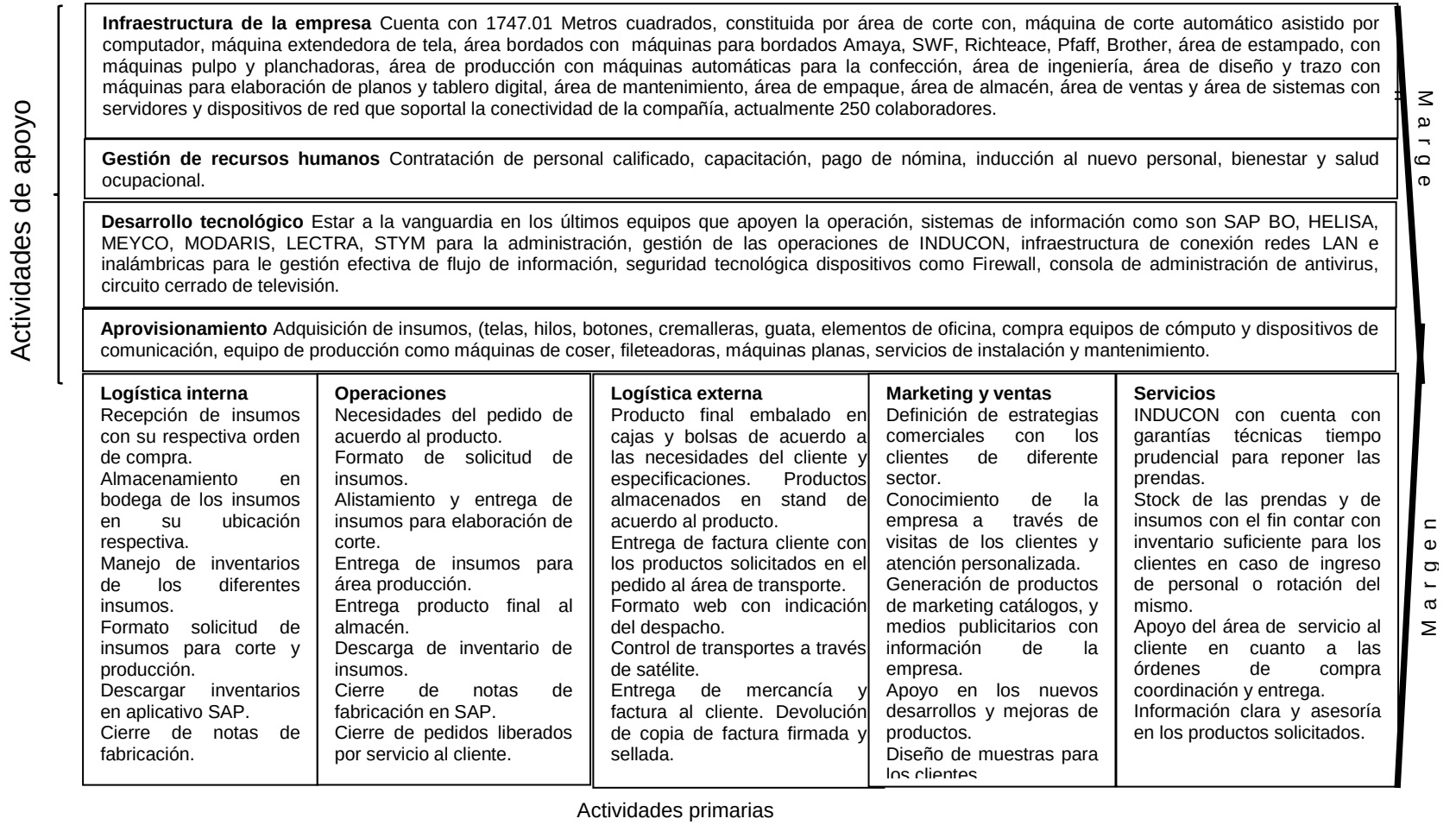
Se establecen pólizas de cumplimiento para garantizar que los productos sean suministrados en los tiempos establecidos y con proveedores específicos se acuerda un rango de precio siempre y cuando exista un acuerdo de negociación con el proveedor. Los proveedores deben cumplir con parámetros de calidad definidos en la ficha técnica de INDUCON, para garantizar la continuidad en la producción.

2.3.1.5 Poder de Negociación de los Clientes. Al tratarse de productos que son de diferentes líneas, se busca satisfacer la necesidad de cada uno de los clientes, los compradores de INDUCON son empresas de diferentes sectores como son industriales, salud, alimentos, sector gobierno, sector estatal entre otras, la rentabilidad en cada uno de estos sectores demuestra un poder de negociación de los compradores bastante alto, debido a que los precios son diferentes en cada uno, excepto en donde se manejan grupos de clientes que buscan un precio en común.

INDUCON es una fábrica que no maneja puntos de venta lo que hace que la negociación sea directa con el comprador. Maneja un cumplimiento alto en las entregas del producto el cual confecciona con excelentes materias primas

independientemente del precio, las prendas se diseñan y se personalizan de acuerdo a las necesidades del cliente, lo cual es una gran ventaja competitiva (véase la Figura 6).

Figura 6. Modelo de la cadena de valor de Porter para INDUCON.



Fuente. Los Autores.

2.3.2 Resumen y Conclusiones del Contexto. Una vez analizado el contexto tanto interno como externo se evidencia que INDUCON cuenta con las siguientes fortalezas: infraestructura tecnológica de TI y sistemas de información actualizados para el desarrollo del diseño y confección de las prendas, su infraestructura física le permiten tener espacios adecuados para el desarrollo de su función y un adecuado desarrollo de la salud ocupacional y condiciones físicas para el trabajador y talento humano comprometido y calificado. La trayectoria de INDUCON, le permite posicionarse dentro del sector de las confecciones como una empresa líder, con buen reconocimiento generando satisfacción con los clientes y proveedores**.**

Así mismo, la organización requiere la implementación de un sistema de gestión de calidad, fijación de políticas de calidad, de seguridad de la información, modelos de gestión enfocada en procesos, definición de manual de funciones por competencias y definición de roles y responsabilidades. Igualmente, requiere un estudio para definir debidamente el contexto externo de la entidad con énfasis en definición de un modelo de estrategias competitivas en el mercado de la confección.

No existe un documento formal de definición de políticas de seguridad de la información, por ende no existe una cultura de seguridad de la información, no existe un modelo de administración por procesos, lo que conlleva a una falta de control, seguimiento de las actividades y que no haya una definición de riesgos por procesos y un mapa de riesgos.

En el área de TI no existen procesos documentados para la transferencia de conocimiento y continuidad en las operaciones normales del área en caso de ausencia de la persona responsable de las actividades de TI, tampoco existen los manuales para usuarios finales alineados con los procesos para el uso adecuado de los aplicativos core del negocio. Necesita herramientas para hacer análisis de mercadotecnia para estudiar futuros clientes y analizar los mismos, esto con el fin de permitir un crecimiento de la organización.

2.3.3 Necesidades y Expectativas en Materia de Seguridad de la Información. Para identificar las necesidades y expectativas de seguridad de la información en INDUCON, se procedió a realizar una reunión con el nivel directivo de la organización, se realizaron entrevistas a funcionarios de los diferentes niveles de la entidad, se diseñó y aplicó una encuesta a los funcionarios del área de TI y de las áreas administrativa, como se videncia en el Anexo A Encuesta seguridad de la información en INDUCON y en el Anexo B Encuesta seguridad de la información en el área de TI.

A continuación se hace referencia a las necesidades y expectativas en materia de seguridad de la información, manifestada por las partes interesadas (véase el Cuadro 4).

Cuadro 4. Necesidades y Expectativas de Seguridad de la Información por las Partes Interesadas de INDUCON

Partes interesadas internas			Partes interesadas externas		
	Necesidades	**Expectativas**		**Necesidades**	**Expectativas**
Gerente	Diseñar un plan de seguridad de la información para el área de TI. Informes para la toma de decisiones. Incremento de las ventas, Buenas relaciones con los proveedores y clientes.	Continuidad en funcionamiento de los sistemas. Solución inmediata a contingencias. Racionalización de los recursos del área de TI.	Proveedores	Mantener buenas relaciones.	Beneficios mutuos y continuidad. Alianza estratégica
Empleados	Capacitación sobre seguridad informática y uso de los aplicativos. Políticas de uso de las TICS. Plan de contingencia de los sistemas de información. Definir roles y responsabilidades. Calidad del ambiente laboral y reconocimiento.	Los sistemas siempre disponibles. Backus de la información. Definición y estandarización de procesos y capacitación.	Clientes	Satisfacción de sus necesidades.	Calidad de los productos. Mejoramiento en la calidad del servicio. .
Dueño	Reducción de costos. Productividad y utilidades.	Productividad. Imagen de la compañía. Rentabilidad y crecimiento de la compañía. La búsqueda de la excelencia de la organización.	Sociedad		Protección ambiental y ética en el negocio. Imagen corporativa
			Gobierno		Cumplimientos de normas legales
			Acreedores		Cumplimiento en pagos y compromisos adquiridos.

Fuente. Los Autores.

2.4 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El alcance del presente proyecto es el diseño del plan de seguridad de la información para el área de TI en INDUCON ubicado en la ciudad de Bogotá, basados en el contexto interno y externo de la organización, en la identificación de necesidades y un análisis de riesgos; con el fin de proporcionarle una herramienta que le permitirá en un futuro la implementación de un SGSI para el área de TI.

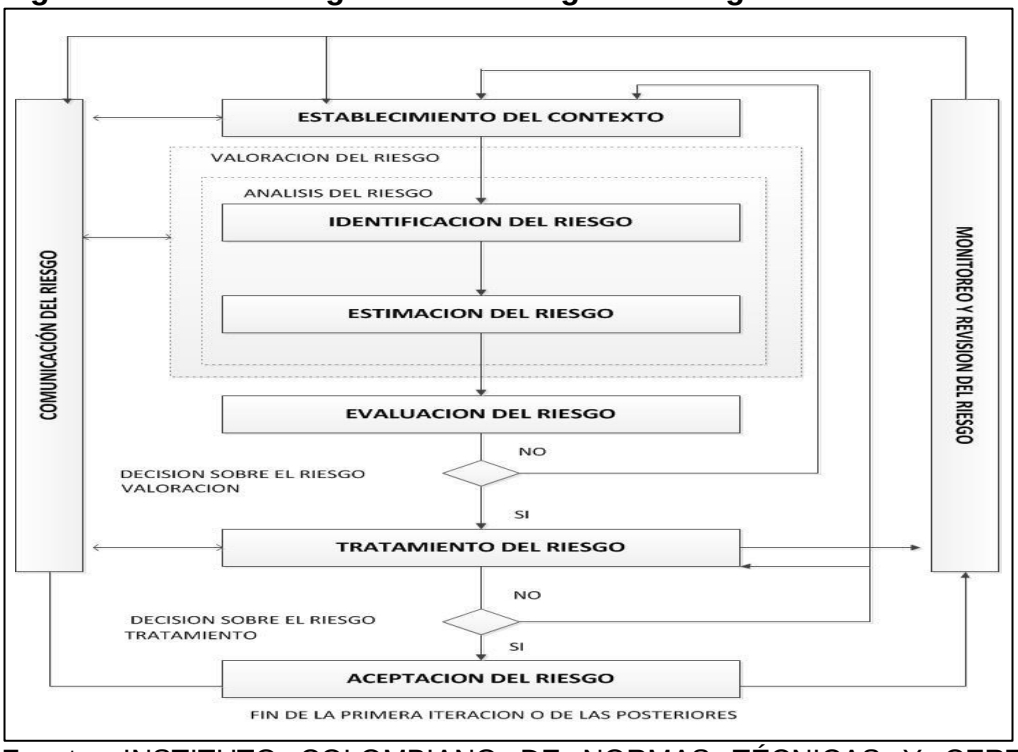
3. METODOLOGÍA DE RIESGOS

La metodología seleccionada para la realización de un plan de seguridad de la información, para el área de TI de la compañía INDUCON, se basa en el estándar de la Norma Técnica Colombiana NTC-ISO/IEC 27005, la cual suministra directrices para la gestión del riesgo en la seguridad de la información, ayudando así a brindar soporte a los requisitos de un sistema de gestión de un SGSI, permitiendo aplicar un método riguroso y comprensivo para describir el comportamiento actual de la compañía y dejar las bases para una implementación de la norma.

3.1 FLUJOGRAMA PARA LOS RIESGOS

Para realizar el flujograma de los riesgos de INDUCON, se toma como base el proceso de gestión del riesgo en la seguridad de la información definido en la Norma Técnica Colombiana NTC-ISO/IEC-27005 (véase la Figura7), el cual define: establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo para efectos del diseño del plan de seguridad de la información del área de TI el cual se desarrollará hasta el tratamiento del riesgo.

Figura 7. Proceso de gestión del riesgo en la seguridad de la información



Fuente. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. p.5

3.2 PARÁMETROS PARA LA GESTIÓN DE RIESGOS

3.2.1 Categorías de Riesgos. Para el diseño del plan de seguridad de la información para el área de TI de la compañía INDUCON, se contempla la siguiente categorización de riesgos (véase el Cuadro 5).

Cuadro 5. Categorización de los Riesgos de INDUCON

Categoría del Riesgo	Descripción	Factores
Económicos	Son los riesgos que se asocian al manejo de los recursos económicos de INDUCON	Presupuesto no definido o insuficiente, para el área de tecnologías de la información.
Humanos	Son los riesgos relacionados con el talento humano de INDUCON	Personal no capacitado en materia de seguridad de la información y ausencia en la organización respecto al tema de la misma.
Tecnológicos	Son los riesgos, asociados con el uso de la tecnología	Obsolescencia, innovación, seguridad en plataforma tecnológica
Naturales	Son los riesgos que contemplan fenómenos naturales	Inundaciones, terremotos, incendios
Gestión y controles	Son los riesgos relacionados con el gobierno de las tecnologías de la información y cumplimiento de normas.	Establecer políticas y usos de la tecnología de la información, nivel de conocimiento de especialistas en temas de Seguridad de la información
Legales	Son los riesgos que tiene INDUCON con la capacidad de cumplir los requisitos legales y contractuales.	Licenciamiento ofimática para el uso del Software en estaciones de trabajo

Fuente. Los Autores.

3.2.2 Definición de la Escala para la Probabilidad. A continuación se muestra como se definió la escala de probabilidad tomando valores cualitativos para el análisis (véase el Cuadro 6).

Cuadro 6. Escala de Probabilidad para los Riesgos de INDUCON

Ítem	Escala		Descripción
1	Muy baja	Muy Improbable	El evento puede ocurrir solo en circunstancias excepcionales
2	Baja	Improbable	El evento puede ocurrir en algún momento
3	Media	Posible	El evento tiene la posibilidad de ocurrir en algún momento
4	Alta	Probables	El evento probablemente ocurrirá en algunas circunstancias
5	Muy alta	Frecuente	Se espera que el evento ocurra en la mayoría de circunstancias

Fuente. Los Autores.

3.2.3 Definición de la Escala de Impacto. Se definió la escala para valorar el impacto y se tomaron valores cualitativos para el análisis (véase el Cuadro 7).

Cuadro 7. Escala de Impacto para los Riesgos de INDUCON

Item	Escala	Descripción
1	Muy baja	Si el hecho llegará a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Baja	Si el hecho llegará a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Media	Si el hecho llegará a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Alta	Si el hecho llegará a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Muy alta	Si el hecho llegará a presentarse, tendría desastrosas consecuencias o efectos en la entidad

Fuente. Los Autores.

3.2.4 Matriz Probabilidad por El impacto. En la siguiente matriz se ilustra la multiplicación de impacto por la probabilidad de ocurrencia (véase el Cuadro 8).

Cuadro 8. Escala de Probabilidad por el Impacto para los Riesgos de INDUCON

Impacto	Probabilidad				
Muy alto (5)	**5**	**10**	**15**	**20**	**25**
Alto (4)	**4**	**8**	**12**	**16**	**20**
Medio (3)	**3**	**6**	**9**	**12**	**15**
Bajo (2)	**2**	**4**	**6**	**8**	**10**
Muy bajo (1)	**1**	**2**	**3**	**4**	**5**
	Muy improbable (1)	Improbable (2)	Posible (3)	Probable (4)	Frecuente (5)

Fuente. Los Autores.

Definición de la zona de tratamiento del riesgo

Riesgos a tratar.

Riesgos que son importantes pero que no afectan la operación de la empresa.

Riesgos que serán aceptados por su mínimo impacto en la operación.

3.2.5 Definición de Criterios para el Tratamiento del Riesgo. En el Cuadro 9 se listan los criterios para el tratamiento del riesgo, y la escala para determinar la aceptación de los riesgos.

Cuadro 9. Criterios para el Tratamiento del Riesgo para INDUCON

Tipo de Riesgo	Escala	Descripción
Riesgo bajo	1-9	Se aceptan pero requieren tratamiento mediante procedimientos rutinarios de gestión de tecnología.
Riego medio	10-15	No se aceptan automáticamente, requieren consulta y atención a nivel de subgerencia y directores quienes determinaran acciones de manejo.
Riesgo alto	16-25	No se aceptan automáticamente, deben ser escalados al nivel de alta gerencia para su evaluación y determinación de la estrategia de manejo.

Fuente. Los Autores.

De acuerdo a los valores obtenidos en el cuadro 6 de probabilidad por el impacto, con los niveles de Alto, medio y bajo, representan el grado o nivel que se encuentran expuestos los activos de TI, igualmente requieren que la gerencia, subgerencia y directores, tomen acción para el logro de los objetivos del área de TI de INDUCON.

Los riesgos evaluados entre 1 y 9 son los que INDUCON aceptará por considerarse que están en un bajo riesgo para las operaciones de la compañía.

Los riesgos evaluados entre 10 y 15 son los que INDUCON aceptará, pero requieren de atención para ser revisados en la siguiente valoración de los riesgos.

Los riesgos evaluados entre 16 y 25 son los que INDUCON debe tratar de acuerdo a la ubicación de esta valoración del Cuadro 8, por considerar que si se materializan esos riesgos impactan fuertemente los objetivos de la empresa.

3.3 OPCIONES DE TRATAMIENTO DEL RIESGO

3.3.1 Transferir. Transferir el riesgo involucra una decisión para compartir algunos riesgos con las partes externas; puede crear nuevos riesgos o modificar los riesgos existentes o identificados.

3.3.2 Aceptarlo. Una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

3.3.3 Mitigarlo. Una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas

3.3.4 Explotar / Compartir. Cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo físico, o parte el mismo a otro sitio.

3.4 CRITERIOS Y ESCALAS PARA VALORACIÓN DE LOS ACTIVOS

Cada activo de información tiene una valoración distinta en la empresa, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información. Pero a la hora de valorarlos, no sólo se tiene en cuenta el costo de adquisición o desarrollo, sino también el costo por la función que desempeña dentro de la organización. Para el caso de estudio se utilizó la valoración cualitativa la cual utiliza términos típicos como:

- Baja.
- Media baja.
- Media.
- Media alta.
- Alta.

Los Cuadros 10, 11, 12, 13, 14, 15 y 16 que se describen a continuación son un insumo para la valoración de activos del Cuadro 17.

A continuación se presenta la valoración del activo imagen empresarial, la cual puede ser afectada por factores tanto internos como externos (véase el Cuadro 10)

Cuadro 10. Imagen Empresarial

Valor Activo	Criterio	Descripción
1	Baja	Leve pérdida de Imagen
2	Media	Pérdida importante de Imagen
3	Alta	Pérdida muy alta de Imagen

Fuente. Los Autores.

Ahora se definen los criterios que afectan la operación normal de la entidad (véase el Cuadro 11).

Cuadro 11. Impacto Operacional

Valor Activo	Criterio	Descripción
1	Baja	Cambios en actividades de rutina.
2	Media baja	No existencia de manuales funcionales.
3	Media	Ausencia de definición de roles, perfiles y responsabilidades.
4	Media alta	No existencia de definición y estandarización de procesos.
5	Alta	Ausencia de políticas de Información y de uso de las TI.

Fuente. Los Autores.

A continuación se definen los criterios que afectarían a la entidad en caso de un incumplimiento legal (véase el Cuadro 12).

Cuadro 12. Cumplimiento Legal

Valor Activo	Criterio	Descripción
1	Baja	Multas por licenciamiento de herramientas ofimáticas.
2	Media	Demandas por liquidación de nomina
3	Alta	Demandas por licenciamiento por los aplicativos core del negocio.

Fuente. Los Autores.

Se definen los criterios de confidencialidad (garantizar que la información solo es conocida por quien está autorizado para conocerla), se define la siguiente escala (véase el Cuadro 13).

Cuadro 13. Matriz de Confidencialidad

Valor Activo	Criterio	Descripción
1	Baja	Información revelada mínima y no secreta
2	Media	Importante cantidad de información no secreta revelada
3	Alta	Toda la información sea revelada

Fuente. Los Autores.

En el Cuadro 14 se definen los criterios de integridad (completitud de la información), se definió la siguiente escala.

Cuadro 14. Matriz de Integridad

Valor Activo	Criterio	Descripción
1	Baja	El daño o modificación no autorizada de información no es crítica para las aplicaciones de la entidad.
2	Media	El daño o modificación no autorizada de información no es crítica pero afecta en forma mínima las aplicaciones de la entidad.
3	Alta	El daño o modificación no autorizada de información es fundamental para las aplicaciones de la entidad

Fuente. Los Autores.

Se definen los criterios de disponibilidad (garantía que la información puede ser accedida por quién la requiere y cuándo la requiere), se definió la siguiente escala (véase el Cuadro 15).

Cuadro 15. Matriz de Disponibilidad

Valor Activo	Criterio	Descripción
1	Baja	Es posible que por un máximo de 7 horas no estén disponibles los sistemas de información de la entidad.
2	Media	Es posible que por un máximo de 3 horas no estén disponibles los sistemas de información de la entidad.
3	Alta	Es posible que por un máximo de 1 hora no estén disponibles los sistemas de información de la entidad.

Fuente. Los Autores.

3.5 IDENTIFICACIÓN DE LOS RIESGOS

Para la identificación de los riesgos, lo primero que se realizará es la identificación de los activos, posteriormente se valorarán estos activos respecto a los criterios de confidencialidad, integridad y disponibilidad de los mismos, y luego se realiza un resumen de los activos con mayor valoración**.**

3.5.1 Identificación de Activos. Debido a que el área de TI se soporta en diferentes servicios y con base al levantamiento de información de la infraestructura tecnológica, de las visitas y entrevistas realizadas a los funcionarios de las diferentes áreas y niveles de la organización, se procedió a identificar y agrupar los activos por categorías, con lo cual, se garantiza un mejor entendimiento de la distribución de los mismos. Los activos identificados se categorizaron en hardware, software, red, personal e instalaciones (véase el Cuadro 16).

Cuadro 16. Identificación de los Activos

Hardware	Descripción
Servidor de aplicaciones y base de datos	Soporta las aplicaciones de SAP Business One, Helisa SGW, Motor base de datos SQL Server 2008.
Servidor de dominio	Soporta el Directorio Activo, recursos compartidos para Modaris, Diamino (aplicativos de diseño).
Estaciones de trabajo de los usuarios	Soporta software ofimático, correo corporativo, aplicación cliente de SAP
Planta telefónica	Comunicación telefónica
Impresoras	Impresión documentos
Medios para datos	Medios de almacenamiento de datos
Software:	**Descripción**
SAP Business One	ERP compuesto por 8 módulos
Modaris	Software de patronaje
Diamino	Software para crear marcadas y colocar las piezas

Cuadro 16. (Continuación)

Software:	Descripción
Helisa SGW	Software contable
Willcom	Software para la realización de bordado
Stym	Métodos y tiempos para producción
Corel Draw 7.0	Aplicativo para diseñar el modelo o la prenda
Sistema Operativo Server	Software que soporta las aplicaciones servidor
Sistema Operativo Cliente	Software que soporta las aplicaciones cliente
Software de ofimática	Software que soporta las actividades diarias.
Software de Base de datos SQL	Soporta los datos de la aplicación SAP
Software colaborativo	Herramienta colaborativa para centralizar las comunicaciones
Correo empresarial	Herramienta de gestión de correos
Red:	**Descripción**
Centro de datos	Alojamiento de equipos activos de red y comunicaciones.
Equipos activos de red	Soportan la comunicación interna y externa de INDUCON
Planta telefónica	Comunicación telefónica
Modem ISP	Router del proveedor del servicio
Routers inalámbricos	Señal inalámbrica
Personal:	**Descripción**
Jefes de oficinas	Personas que toman decisiones
Usuarios	Usuarios de las diferentes aplicaciones
Personal de operación/ mantenimiento	Administración y control de las aplicaciones, copias de seguridad, mesa de ayuda.
Instalaciones:	Descripción
Centro de cómputo	Acceso controlado para el ingreso mediante seguro de puerta.

Fuente. Los Autores.

3.5.2 Valoración de Activos Bajo Criterios de Confidencialidad, Integridad y Disponibilidad. La valoración de los activos es necesario realizarla en función de la relevancia que estos tengan para la empresa y del impacto que una incidencia sobre el mismo pueda causar a la entidad y que afecte la confidencialidad, integridad y disponibilidad (véase el Cuadro 17).

Se utilizaron las escalas para valoración de los activos definidos en el numeral 3.4 de este documento.

Cuadro 17. Matriz Valoración de Activos

		Valor			∑
Hardware	**Descripción**	**C**	**I**	**D**	**C+I+D**
Servidor de aplicaciones y base de datos.	Soporta las aplicaciones de SAP Business One, Helisa SGW, Motor base de datos SQL Server 2008.	3	3	3	**9**
Servidor de dominio.	Soporta el Directorio Activo, recursos compartidos para Modaris, Diamino (aplicativos de diseño).	3	2	3	**8**
Estaciones de trabajo de los usuarios.	Soporta software ofimático, correo corporativo, aplicación cliente de SAP.	1	0	3	**4**
Planta telefónica.	Comunicación telefónica.	0	0	2	**2**
Impresoras.	Impresión documentos.	0	0	1	**1**
Medios para datos.	Medios de almacenamiento de datos.	2	3	3	**8**
Software:	**Descripción**				
SAP Business One.	ERP compuesto por 8 módulos.	3	3	3	**9**
Modaris.	Software de patronaje.	1	3	2	**6**
Diamino.	Software para crear marcadas y colocar las piezas.	1	3	2	**6**
Helisa SGW.	Software contable.	2	3	2	**7**
Willcom.	Software para la realización de bordado.	1	3	2	**6**
Stym.	Métodos y tiempos para producción.	2	3	3	**8**
Corel Draw 7.0.	Aplicativo para diseñar el modelo o la prenda.	1	3	1	**5**
Sistema operativo server.	Software que soporta las aplicaciones servidor.	3	3	3	**9**
Sistema operativo cliente.	Software que soporta las aplicaciones cliente.	3	3	1	**7**
Software de ofimática.	Software que soporta las actividades diarias.	3	3	1	**7**
Software de base de datos SQL.	Soporta los datos de la aplicación SAP.	3	3	3	**9**
Software colaborativo.	Herramienta colaborativa para centralizar las comunicaciones.	3	1	1	**5**
Correo empresarial.	Herramienta de gestión de correos.	3	1	1	**5**
Personal:	**Descripción**				
Administrador de Base de Datos.	Responsable de la administración, control y monitoreo de la base de datos.	3	3	2	**8**
Soporte nivel 1 ofimática, hardware.	Responsable de soporte a usuario final.	2	2	1	**5**
Soporte aplicaciones.	Responsable de soporte a usuario final.	3	2	3	**8**
Mesa de ayuda.	Responsable de atender los requerimientos de acuerdo a la solicitud.	0	0	1	**1**
Administrador de red.	Responsable del funcionamiento de la arquitectura de red.	2	2	2	**6**
Administrador de la seguridad.	Responsable de la seguridad de la información.	3	2	3	**8**
Red:	**Descripción**				
Centro de datos.	Alojamiento de equipos activos de red y comunicaciones.	0	0	3	**3**
Equipos activos de red.	Soportan la comunicación interna y externa de INDUCON.	0	0	3	**3**
Planta telefónica.	Comunicación telefónica.	0	0	2	**2**
Modem ISP.	Router del proveedor del servicio.	0	0	3	**3**
Routers inalámbricos.	Señal inalámbrica.	0	0	1	**1**

Fuente. Los Autores.

En el Cuadro 17, se relacionan los activos de TI, que arrojaron un impacto alto de riesgo, por lo tanto deben ser tratados. El impacto alto está definido por la sumatoria de la confidencialidad, integridad y disponibilidad cuyos valores están entre cinco y nueve.

A continuación se listan los activos a tratar, por su alto impacto en la confidencialidad, integridad y disponibilidad (véase el Cuadro 18).

Cuadro 18. Resumen de los Activos

Activo	Descripción	C	I	D	∑
Servidor de aplicaciones y base de datos.	Soporta las aplicaciones de SAP Business One, Helisa SGW, Motor base de datos SQL Server 2008.	3	3	3	**9**
Software de Base de datos SQL.	Soporta los datos de la aplicación SAP.	3	3	3	**9**
SAP Business One.	ERP compuesto por 8 módulos.	3	3	3	**9**
Sistema operativo server.	Software que soporta las aplicaciones servidor.	3	3	3	**9**
Administrador de base de datos.	Responsable de la administración, control y monitoreo de la base de datos.	3	3	2	**8**
Medios para datos.	Medios de almacenamiento de datos.	2	3	3	**8**
Servidor de dominio.	Soporta el Directorio Activo, recursos compartidos para Modaris, Diamino (aplicativos de diseño).	3	2	3	**8**
Stym.	Métodos y tiempos para producción.	2	3	3	**8**
Soporte aplicaciones.	Responsable de soporte a usuario final.	3	2	3	**8**
Administrador de la seguridad.	Responsable de la seguridad de la información.	3	2	3	**8**
Helisa SGW.	Software contable.	2	3	2	**7**
Sistema operativo cliente.	Software que soporta las aplicaciones cliente.	3	3	1	**7**
Software de ofimática.	Software que soporta las actividades diarias.	3	3	1	**7**
Administrador de red.	Responsable del funcionamiento de la arquitectura de red.	2	2	2	**6**
Modaris.	Software de patronaje.	1	3	2	**6**
Diamino.	Software para crear marcadas y colocar las piezas.	1	3	2	**6**
Willcom.	Software para la realización de bordado.	1	3	2	**6**
Corel Draw 7.0.	Aplicativo para diseñar el modelo o la prenda.	1	3	1	**5**
Software colaborativo.	Herramienta colaborativa para centralizar las comunicaciones.	3	1	1	**5**
Correo empresarial.	Herramienta de gestión de correos.	3	1	1	**5**

Fuente. Los Autores.

3.5.3 Identificación de Amenazas. Una vez identificado los activos en los cuales el valor es más alto de acuerdo con su confidencialidad, integridad y disponibilidad, a continuación se identifican las amenazas que son críticas para cada uno de ellos, con el fin de mitigar el impacto de ocurrencia en los activos (véase el Cuadro 19). En el Anexo C. Se enumera el listado completo de amenazas.

Para la identificación de las amenazas se utilizó la información obtenida en las entrevistas y encuestas realizadas a los funcionarios de los diferentes niveles de INDUCON, apoyados en la norma técnica NTC-ISO/IEC Colombiana 27005 y la experiencia profesional de los realizadores de este proyecto.

Cuadro 19. Amenazas Críticas

Activo	Amenaza
Servidor de aplicaciones y base de datos.	Daño físico. Daño lógico. Software malicioso. Mal funcionamiento del software. Uso no autorizado del equipo. Espionaje remoto. Eventos naturales. Susceptibilidad a las variaciones de voltaje. Susceptibilidad a las variaciones de temperatura.
Software de base de datos SQL.	Errores de mantenimiento / actualización de software. Mala gestión de directivas de seguridad. Principios de privilegios mínimos(*). Validación de boletines de seguridad(**). Validación de los puertos de red(***) Configuración incorrecta de las cuentas de servicio.
SAP Business One.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos). Errores de mantenimiento / actualización de programas.
	Mala aplicación de un parche. Falta del manual de usuario para el manejo de la aplicación. Errores del administrador. Errores de configuración. Defectos en el código de los programas. Caída del sistema por agotamiento de recursos. Abuso de privilegios. Administración deficiente de los usuarios con acceso al sistema.
Sistema operativo server.	Errores de mantenimiento / actualización de software. Espionaje remoto. Malware (Virus, spyware). Avería de origen físico / lógico. Errores de monitorización (log). Caída del sistema por agotamiento de recursos. Administración deficiente de los usuarios con acceso al sistema. Administración deficiente de políticas de contraseña.
Administrador de base de datos.	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. Uso inadecuado de procedimientos en la base de datos.
Medios para datos.	Daño físico. Daño lógico.
Servidor de dominio.	Daño Físico. Falla suministro de energía. Falla técnica. Mal funcionamiento del equipo.

(*)Principio de privilegios mínimos un sistema solo debería permitir un nivel de acceso necesario a un objeto protegible y debe estar habilitado para los que tienen una necesidad directa y solo por un tiempo específico.
(**)Boletines de seguridad se deben validar los boletines de seguridad que son emitidos por las entidades donde ya fueron probados y validados con el fin de no poner en peligro al sistema por no implementarlo
(***)Validación puertos de red, puertos estándar que estén abiertos a internet se puede presentar un ataque.

Cuadro 19. (Continuación)

Activo	Amenaza
	Software malicioso. Daño lógico. Eventos naturales. Actualización sin supervisión. Susceptibilidad a las variaciones de temperatura.
Stym.	Obsolescencia en las herramientas de desarrollo. Mala aplicación de un parche. Errores de configuración. Administración deficiente de políticas de contraseña. Administración deficiente de los usuarios con acceso al sistema.
Soporte aplicaciones.	Conocimiento insuficiente del funcionamiento de la aplicación. Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. No definición de roles.
Administrador de seguridad.	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. Error en el uso. Realizar pruebas en ambientes de producción. Uso excesivo de restricciones para el uso del sistema.
Helisa SGW.	Errores de mantenimiento / actualización de programas. Administración deficiente de los usuarios con acceso al sistema.
Sistema operativo cliente.	Errores de mantenimiento / actualización de software. Espionaje remoto. Malware (Virus, spyware) Avería de origen físico / lógico Manipulación errónea de la configuración del equipo.
Software de ofimática.	Errores de mantenimiento / actualización de software. Software no licenciado. Error de usuario (borrado de archivos)
Administrador de red.	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. Falta de conocimiento en la integración de redes. Falta de monitorización de los registros de log de los dispositivos de red.
Modaris.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos). Mala aplicación de un parche. Errores de configuración. Caída del sistema por agotamiento de recursos.
Diamino.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos). Errores de mantenimiento / actualización de programas. Caída del sistema por agotamiento de recursos.
Willcom.	Falta de monitorización por estar instalado en la estación del usuario que lo maneja. Manipulación con software.
Corel Draw 7.0.	Errores de mantenimiento / actualización de programas.
Software colaborativo.	Errores de mantenimiento / actualización de software. Principio de privilegios mínimos.
	Administración deficiente de los usuarios con acceso al sistema. Validación de puertos de la aplicación(*)
Correo empresarial.	Uso inadecuado del correo. Descarga de contenido como virus, gusanos y todo clase malware. Demora en la atención de solicitudes por falla en la plataforma.

Fuente. Los Autores.

(*)Validación puertos de red, puertos estándar que estén abiertos a internet se puede presentar un ataque

3.5.4 Identificación de Vulnerabilidades. Para identificar las vulnerabilidades se utiliza un modelo de alto nivel que permite abordar una visión más global de la organización y su sistema de información, tomando como punto de referencia el análisis del contexto interno y externo de INDUCON concentrándonos más en el negocio, y determinando así los activos más relevantes.

Se procede a identificar un listado de amenazas y vulnerabilidades para cada activo de la organización y nos centramos en validar los más críticos, agrupados en un dominio y finalmente seleccionar los objetivos de control específicos que ayuden a mitigar esos riesgos, buscando un enfoque sencillo que facilite la aceptación de un plan de trabajo para la valoración de riesgos, minimizar los recursos económicos, y aplicarlos donde así se consideren necesarios y se obtenga un mayor beneficio en la necesidad de protección.

En el Cuadro 20 se numeran las vulnerabilidades encontradas.

Cuadro 20. Identificación de Vulnerabilidades

Activo	Vulnerabilidades
Hardware.	Mantenimiento insuficiente / Instalación fallida de parches y actualizaciones. Ausencia de un eficiente control de cambio en la configuración. Backup o copia no controlada. Falta de concientización de los usuarios. Falta de gestión de capacidad. Falta de mantenimiento físico /lógico. Ausencia de planes de contingencia. Falta de mantenimiento planificado de los elementos de soporte. Obsolescencia de hardware. Falta de gestión adecuada de herramientas y registros de auditoría.
Software.	Ausencia o insuficiencia de pruebas de software. Ausencia de terminación de la sesión cuando se abandona la estación de trabajo. Interfaz de usuario compleja. Ausencia de documentación. Configuración incorrecta de parámetros. Gestión deficiente de las contraseñas. Falta de gestión de acceso de usuarios.
Software.	Falta de política de pantalla limpia. Ausencia de revisión de manuales. Inadecuada definición de roles y responsabilidades. Falta de procedimientos de identificación y clasificación de la información.
	Faltan esquemas de gestión de cambios. Falta un adecuado manejo de versiones. Falta de capacitación de personal. Falla en la segregación de ambientes de producción, desarrollo y pruebas. Inadecuados esquemas de almacenamiento de licencias. Falta del manual de usuario para el manejo de la aplicación. Entrenamiento insuficiente en seguridad.

Cuadro 20. (Continuación)

Activo	Vulnerabilidades
Red.	Conexión deficiente de los cables. Transferencia de contraseñas en claro. Mala parametrización en los dispositivos de red. Falta de planes de contingencia. Ausencia de monitoreo de la red. Control de capacidad para el almacenamiento. Ubicación de sitios deficientes en seguridad física (sitios sin control de acceso). Falta capacitación de usuarios. Obsolescencia. Falta de seguimiento de normas para la implementación de un centro de datos. Falta de gestión de cambios. Administración deficiente de políticas de contraseña. Protección física inadecuada. Falta de un plan de continuidad. Sistemas de detección y extinción de incendios inadecuado.
Personal.	Ausencia de personal. Entrenamiento insuficiente en seguridad. Uso incorrecto de software y hardware. Falta de conciencia acerca de la seguridad. Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería. Procesos de revisión inexistentes. Falta de gestión de acceso a usuarios. Falta de concientización de terceros en seguridad de la información. Falta de un plan de continuidad. Resistencia a la cultura en seguridad de la información. Falta de un esquema de respaldo a nivel de funciones / conocimiento.
Lugar.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y oficinas.
Organización.	Ausencia de procedimiento formal para el registro y retiro de usuarios. Ausencia de procedimientos de identificación y valoración de riesgos. Ausencia en el procedimiento de control de cambios.
	Ausencia de procedimiento formal para el control de la documentación de un SGSI. Ausencia de asignación adecuada de responsabilidades en la seguridad de la información. Ausencia de planes de continuidad. Ausencia de procedimientos de clasificación para el manejo de información. Ausencia de procedimientos formales en la organización. Ausencia de manuales de funciones de definición de responsabilidades y roles en el área de TI.

Fuente. Los Autores.

3.5.5 Resumen. De acuerdo al anterior grupo de activos se evidencia el alto grado de vulnerabilidades que están sometidos los activos de TI, recurso humano y la organización, donde se evidencia que la mayoría de vulnerabilidades son por la ausencia de procedimientos para la gestión adecuada de TI, la falta de

concientización en seguridad de la información, el uso inadecuado de los sistemas de información, la falta de capacitación en temas de seguridad como también una correcta definición de roles y responsabilidades. Sin descuidar que los recursos tecnológicos como son el hardware y software son fundamentales y toman un papel importante en las actividades que se realizan día a día en la empresa.

Todas estas vulnerabilidades deben ser tratadas y minimizadas con el fin de ayudar a INDUCON a mitigar los riesgos.

3.6 MATRIZ DE RIESGOS

Una vez definidos los activos, valorados sus riesgos frente a los criterios definidos se procede a realizar la matriz de riesgos, donde se define el activo, el riesgo asociado y se genera el nivel del riesgo al cual están expuestos los activos, valorando la probabilidad por el impacto para cada uno de los activos, el resultado del nivel es calculado tomando la escala de la probabilidad para cada riesgo que se obtiene del Cuadro 6 y multiplicándolo por los valores del Cuadro 7 que corresponde al impacto.

Para determinar los valores de la escala de probabilidad fue necesario realizar una entrevista con el Ingeniero de sistemas de la empresa, evaluando cada uno de los riesgos asociados, su frecuencia y probabilidad de ocurrencia de la misma, la escala toma unos valores de 1 a 5 siendo uno (1) muy bajo; donde el incidente puede ocurrir en una circunstancia excepcional, en cambio el calificativo de cinco (5) se espera que el incidente ocurra en la mayoría de circunstancias.

Para determinar los valores de la escala del impacto que define la materialización de un riesgo o amenaza, se realiza entrevista con el Ingeniero de sistemas preguntándole ¿qué pasaría en un determinado momento, y que tan crítico sería que una de las amenazas del cuadro 19 se materialice?, se define una escala donde el valor menos representativo es uno (1); donde se afirma que si el hecho llegará a presentarse tendría consecuencias o efectos mínimos para la empresa, por el contrario si la escala es de cinco (5), tendría desastrosas consecuencias o efectos para la entidad.

En el Cuadro 21 se procede a evaluar los resultados de la probabilidad por el impacto.

Cuadro 21. Matriz de Riesgos

Activo	Riesgo asociado	Probabilidad	Impacto	Nivel
Servidor de aplicaciones y base de datos.	Daño físico.	4	5	20
	Daño lógico.	4	5	20
	Software malicioso.	3	4	12
	Mal funcionamiento del software.	3	5	15
	Uso no autorizado del equipo.	2	4	8
	Espionaje remoto.	3	5	15
	Eventos naturales.	1	5	5
	Susceptibilidad a las variaciones de voltaje.	2	5	10
	Susceptibilidad a las variaciones de temperatura.	2	5	10
Software de Base de datos SQL.	Validación de los puertos de red.	3	5	15
	Errores de mantenimiento / actualización de software.	4	5	20
	Mala gestión de directivas de seguridad.	4	5	20
	Principios de privilegios mínimos.	4	5	20
	Validación de boletines de seguridad.	3	4	12
	Configuración incorrecta de las cuentas de servicio.	3	4	12
SAP Business One.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos).	3	5	15
	Errores de mantenimiento / actualización de programas.	3	5	15
	Mala aplicación de un parche.	3	5	15
	Falta del manual de usuario para el manejo de la aplicación.	5	2	10
	Errores del administrador.	3	5	15
	Errores de configuración.	3	5	15
	Defectos en el código de los programas.	3	5	15
	Caída del sistema por agotamiento de recursos.	3	5	15
SAP Business One.	Abuso de privilegios.	4	5	20
	Administración deficiente de los usuarios con acceso al sistema.	4	5	20

Cuadro 21. (Continuación)

Activo	Riesgo asociado	Probabilidad	Impacto	Nivel
Sistema Operativo Server.	Errores de mantenimiento / actualización de software.	2	4	8
	Espionaje remoto.	3	4	12
	Malware (Virus, spyware).	3	5	15
	Avería de origen físico / lógico.	3	5	15
	Errores de monitorización (log).	2	4	8
	Caída del sistema por agotamiento de recursos.	3	4	12
	Administración deficiente de los usuarios con acceso al sistema.	3	5	15
	Administración deficiente de políticas de contraseña.	4	5	20
Administrador de Base de Datos.	Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.	4	5	20
	Uso inadecuado de procedimientos en la base de datos.	3	5	15
Medios para datos.	Daño físico.	3	5	15
	Daño lógico.	3	5	15
Servidor de dominio.	Daño físico.	3	5	15
	Falla suministro de energía.	3	4	12
	Falla técnica.	3	5	15
	Mal funcionamiento del equipo.	3	5	15
	Software malicioso.	2	4	8
	Daño lógico.	3	5	15
	Eventos naturales.	1	5	5
	Actualización sin supervisión.	2	4	8
	Administración deficiente de políticas de contraseña.	4	5	20
Soporte aplicaciones.	Conocimiento insuficiente del funcionamiento de la aplicación.	3	5	15
	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.	3	5	15
	No definición de roles.	4	5	20

Cuadro 21. (Continuación)

Activo	Riesgo asociado	Probabilidad	Impacto	Nivel
Administrador de seguridad.	Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.	3	5	15
	Persona no capacitada.	4	5	20
	Realizar pruebas en ambientes de producción.	3	5	15
	Uso excesivo de restricciones para el uso del sistema.	3	4	12
	No definición de roles.	4	5	20
Administrador de red.	Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.	3	5	15
	Falta de conocimiento en la integración de redes.	3	5	15
	Falta de monitorización de los registros de log de los dispositivos de red.	3	4	12
	No definición de roles.	4	5	20
Helisa SGW.	Errores de mantenimiento / actualización de programas.	2	3	6
	Falta del manual de usuario para el manejo de la aplicación.	5	3	15
	Administración deficiente de los usuarios con acceso al sistema.	3	3	9
Stym.	Obsolescencia en las herramientas de desarrollo.	4	3	12
	Falta del manual de usuario para el manejo de la aplicación.	5	4	20
	Mala aplicación de un parche.	3	5	15
	Errores de configuración.	3	5	15
Stym.	Administración deficiente de políticas de contraseña.	5	4	20
	Administración deficiente de los usuarios con acceso al sistema.	3	4	12
Sistema Operativo Cliente.	Errores de mantenimiento / actualización de software.	2	3	6
	Espionaje remoto.	3	4	12
	Malware (Virus, spyware).	3	4	12
	Avería de origen físico / lógico.	3	5	15
	Manipulación errónea de la configuración del equipo.	2	4	8

Cuadro 21. (Continuación)

Activo	Riesgo asociado	Probabilidad	Impacto	Nivel
Software de ofimática.	Errores de mantenimiento / actualización de software.	2	3	6
	Software no licenciado.	4	5	20
	Error de usuario (borrado de archivos)	3	4	12
Modaris.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos).	3	4	12
	Mala aplicación de un parche.	3	4	12
	Errores de configuración.	2	4	8
	Caída del sistema por agotamiento de recursos.	3	4	12
Diamino.	Errores de los usuarios (Equivocaciones de las personas en la captura de datos).	3	4	12
	Errores de mantenimiento / actualización de programas.	2	3	6
	Caída del sistema por agotamiento de recursos.	2	3	6
Willcom.	Falta de monitorización por estar instalado en la estación del usuario que lo maneja.	3	5	15
	Manipulación con software.	4	5	20
Corel Draw 7.0.	Errores de mantenimiento / actualización de programas.	3	4	12
Software colaborativo.	Errores de mantenimiento / actualización de software.	2	3	6
	Principio de privilegios mínimos.	2	3	6
Software colaborativo.	Administración deficiente de los usuarios con acceso al sistema.	2	3	6
	Validación de puertos de la aplicación.	2	4	8
Correo empresarial.	Uso inadecuado del correo.	4	5	20
	Descarga de contenido como virus, gusanos y todo clase malware.	4	5	20
	Demora en la atención de solicitudes por falla en la plataforma.	2	4	8

Fuente. Los Autores.

4. PLAN DE TRATAMIENTO DEL RIESGO

Una vez realizada la valoración de los riesgos de los activos, se procede a realizar el resumen de los riesgos que se tratarán según la valoración definida en el Cuadro 22.

Cuadro 22. Resumen de Riesgos a Tratar

No.	Riesgos
1	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.
2	No definición de roles.
3	Persona no capacitada.
4	Uso inadecuado del correo.
5	Descarga de contenido como virus, gusanos y todo clase malware.
6	Administración deficiente de los usuarios con acceso al sistema.
7	Abuso de privilegios.
8	Falta del manual de usuario para el manejo de la aplicación.
9	Daño físico.
10	Daño lógico.
11	Administración deficiente de políticas de contraseña.
12	Mala gestión de directivas de seguridad.
13	Errores de mantenimiento / actualización de software.
14	Principios de privilegios mínimos.
15	Software no licenciado.
16	No existe Backup.

Fuente. Los Autores.

4.1 PLAN DE TRATAMIENTO DEL RIESGO

Para realizar el tratamiento de los riesgos evaluados se agruparon los activos y sus riesgos por el control que se puede aplicar a varios de ellos, de igual manera, se agruparon por tipo de riesgo con la finalidad de reducir el número de planes a implementar en el área de TI; Todas las políticas que se generen en este plan de tratamiento del riesgo deben ser aprobadas por la alta Gerencia de INDUCON, mediante un acto administrativo. A continuación se enumeran los diferentes planes de tratamiento de los riesgos (véase el Cuadro 23).

Cuadro 23. Plan de Tratamiento del Riesgo Número 1 Enunciado en el Cuadro 22

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
1	No disponibilidad del personal (ausencia accidental del puesto de trabajo: enfermedad, alteración del orden público)	A.6.1	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contacto apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
		A.7.1	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Recursos

Humanos:

Talento humano: Una persona para redacción y revisión de los acuerdos de niveles de servicio para los funcionarios, los proveedores de los sistemas de información de INDUCON y de los contratistas.

Especialista seguridad información: Se requiere de un Especialista en seguridad informática por dos días para redacción de los acuerdos de niveles de servicio para los funcionarios, los proveedores de los sistemas de información de INDUCON y de los contratistas y revisión del plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs. De acuerdo al conocimiento y mercado actual puede considerarse un valor aprox. por su servicio de consultoría por valor hora de $50.000

Ingeniero de sistemas: Se requiere un Ing., de sistemas de 4 a 5 semanas aproximadamente para definir y documentar el plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs. De acuerdo al conocimiento y mercado actual puede considerarse un valor aprox mensual. de $3.000.000
Gerente General: Para la aprobación el plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs y de los acuerdos de niveles de servicio.
Abogado: Persona jurídica para la revisión de condiciones de los acuerdos de niveles de servicio.

Acciones

Capacitar como mínimo a dos personas en las actividades del área de TI, para que siempre exista una persona backup en caso de enfermedad del titular u otra eventualidad.

Mantener listado actualizado con nombres, número de teléfono, correo y redes sociales de los responsables del área de TI, del área de Seguridad de la información, de los proveedores o responsables de la tecnología y los sistemas de INDUCON.
Redactar los acuerdos de niveles de servicio para los funcionarios, los proveedores de los sistemas de información de INDUCON y de los contratistas, respecto a disponibilidad de los sistemas de información y la de tecnología.

Cuadro 23. (Continuación)

Acciones					
Definir y documentar el plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs, de INDUCON. Aprobación del plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs, por parte de la gerencia de INDUCON. Capacitación y sensibilización para dar a conocer plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs todo los nivel de la organización. Realizar simulacros y monitorear la aplicación plan de contingencias de Tecnologías de la Información y Comunicaciones – TICs.					
Cronograma propuesto de implementación					
Nro. Acción	**Responsable**	**Fecha Inicio**	**Fecha Fin**	**Fecha Seguimiento**	**Responsable de seguimiento**
1.	Administrador de Sistemas	03/11/2015	17/11/2015	Semestral	Especialista de seguridad de la información.
2	Ingeniero de sistemas	03/11/2015	05/11/2015	09/11/2015	Especialista de seguridad de la información.
3.	Talento humano, Especialista de seguridad de la información y Abogado	04/11/2015	13/11/2015	17/11/2015	Especialista de seguridad de la información.
4.	Ingeniero de Sistemas	18/11/2015	24/11/2015	30/11/2015	Especialista de seguridad de la información.
5.	Gerente General	26/11/2015	28/11/2015	28/11/2015	Ingeniero de Sistemas.
6.	Ingeniero de sistemas	02/12/2015	02/12/2015	Semestral	Ingeniero de Sistemas
7.	Ingeniero de sistemas, administrador de sistemas	20/01/2016	20/01/2016	Semestral	Especialista de seguridad de la información.
Observaciones.					

Fuente. Los Autores.

Cuadro 24. Plan de Tratamiento del Riesgo Número 2 Enunciado en el Cuadro 22.

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
2	No definición de roles.	A.6.1	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	A.6.1.1	Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

Recursos

Humanos: Jefes de áreas de INDUCON: Asignar roles y responsabilidades a los funcionarios que accedan a los sistemas de información de INDUCON.
Talento humano: Una persona por un día cada seis meses para capacitación y sensibilización en seguridad de la información a los funcionarios de INDUCON.
Especialista seguridad información: Realizar acompañamiento y supervisión en la asignación de usuarios de acuerdo a los roles. De acuerdo al conocimiento y mercado actual puede considerarse un valor aprox. por su servicio por valor mensual de $3.500.000
Administrador de Sistemas: Se requiere un Administrador del sistema para creación del usuario en el sistema, con los roles y perfiles solicitados por el jefe de área. De acuerdo al mercado y conocimientos específicos puede considerarse un valor aprox. de 2.500.000
Ingeniero de Sistemas: se requiere un Ing. de Sistemas para realizar auditorías para el seguimiento de la asignación de roles. De acuerdo al conocimiento y mercado actual puede considerarse un valor mensual aprox. de $3.000.000

Acciones

Definir y asignar los roles y responsabilidades teniendo en cuenta las políticas de la seguridad de la información.
Capacitar a los coordinadores de áreas respecto a definición de roles y responsabilidades de los usuarios que acceden a los sistemas de información de INDUCON.
Identificar, definir los activos y los procesos de seguridad de la información.
Definir y documentar los niveles de autorización.
Creación de los usuarios de acuerdo a los roles definidos
Capacitar y sensibilizar a los funcionarios de INDUCON en seguridad de la información.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Jefes de área	03/11/2015	17/11/2015	Semestral	Especialista de seguridad de la información o Ingeniero de sistemas.
2	Ingeniero de Sistemas	04/11/2015	05/11/2015	09/11/2015	Especialista de seguridad de la información.
3.	Especialista de seguridad de la información, Ingeniero de Sistemas y Jefes de área.	06/11/2015	14/12/2015	04/12/2015	Especialista de seguridad de la información.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
4.	Administrador de Sistemas	04/01/2016	22/01/2016	25/01/2016	Especialista de seguridad de la información.
5.	Administrador de Sistemas	26/01/2016	28/01/2016	01/02/2016	Ingeniero de Sistemas.
6.	Talento Humano	10/11/2015	11/11/2015	Semestral	Ingeniero de Sistemas

Observaciones

Fuente. Los Autores.

Cuadro 25. Plan de Tratamiento del Riesgo Número 3 y 12 Enunciados en el Cuadro 22

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
3 12	Persona no capacitada. Mala gestión de directivas de seguridad.	A.7.1	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
			.	A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
		A.5.1	Brindar orientación y soporte por parte de la Dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos.	A.5.1.1	Políticas para la seguridad de la información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes pertinentes.

Recursos

Humanos:

Talento humano: Definir el manual de funciones por competencias y los requisitos para los cargos, verificar las certificaciones, referencias de experiencia y recomendaciones presentadas por los candidatos al cargo, verificación de antecedentes penales y definición de acuerdos contractuales con empleados y contratistas.

Una persona de Talento Humano para apoyo en revisión y redacción de la política de seguridad de la información.

Especialista seguridad información: se requiere de un Especialista en Seguridad Informática que participe en la definición del manual de funciones por competencias y requisitos para los cargos del área de TI y de acuerdos contractuales con empleados y contratistas. Un día para redacción de la política de seguridad de la información. De acuerdo al mercado y conocimiento puede considerarse un valor mensual de $3.500.000

Ingeniero de Sistemas: Se requiere de un Ing. de Sistemas para participar en la definición del manual de funciones por competencias y requisitos para los cargos del área de TI y de acuerdos contractuales con empleados y contratistas. Capacitar y monitorear la aplicación de las políticas y procedimientos de seguridad de la información. De acuerdo al mercado, perfil y conocimiento se puede asignar un valor mensual de 3.000.000

Gerente General: Para la aprobación y revisión del manual de funciones y acuerdos contractuales con empleados y contratistas. Aprobación de la política de seguridad de la información.

Abogado: Persona jurídica para la revisión del manual de funciones y acuerdos contractuales con empleados y contratistas. Revisar la política de seguridad de la información y su pertinencia legal.

Cuadro 25. (Continuación)

Acciones

Definir y elaborar el manual de funciones por competencias y los requisitos para los cargos, verificar las certificaciones, referencias de experiencia y recomendaciones presentadas por los candidatos al cargo, verificación de antecedentes penales y definición de acuerdos contractuales con empleados y contratistas.

Participar en la definición del manual de funciones por competencias y requisitos para los cargos del área de TI y de acuerdos contractuales con empleados y contratistas.

Revisión y aprobación del manual de funciones y acuerdos contractuales con empleados y contratistas

Aplicar y exigir el cumplimiento de las políticas de seguridad de la información, las cuales ya están aprobadas por la Gerencia de INDUCON, y es conocida por todos los funcionaros porque gestión humana e Ingeniero de Sistemas ya capacitaron al respecto.

Redactar las políticas para la seguridad de la información con base en los requisitos del negocio.
Aprobación de la política por parte de la gerencia de INDUCON.

Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Gestión Humana Abogado	03/11/2015	08/01/2016	12/01/2016	Jefe de Gestión Humana, Especialista de seguridad de la información
2	Especialista de seguridad de la información Ingeniero de sistemas	03/11/2015	08/01/2016	12/01/2016	Jefe de Gestión Humana Especialista de seguridad de la información.
3.	Gerente	18/01/2016	02/02/2016	05/02/2016	Jefe de Gestión Humana.
4.	Ingeniero de Sistemas	18/11/2015	24/11/2015	30/11/2015	Especialista de seguridad de la información.|
5	Especialista de seguridad de la información	01/09/2015	03/09/2015	Semestral	Especialista de seguridad de la información.
6	Gerente general	04/09/2015	04/09/2015	05/09/2015	Especialista de seguridad de la información.
7	Ingeniero de sistemas Talento Humano	15/09/2015	16/09/2015	18/09/2015	Especialista de seguridad de la información.
8	Ingeniero de sistemas	26/09/2015	Continua	Semestral	Especialista de seguridad de la información.

Observaciones

Fuente. Los Autores

Cuadro 26. Plan de Tratamiento de los Riesgos Números 4 y 5 Enunciados en el Cuadro 22

Riesgo		Objetivo De Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
4 5	Uso inadecuado del correo. Descarga de contenido como virus, gusanos y todo clase malware.	A.5.1	Brindar orientación y soporte por parte de la Dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	A.5.1.1	Políticas para la seguridad de la información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes pertinentes.
		A.12.2.	Asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso	A.12.2.1	Controles contra código malicioso.	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
		A.13.2	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.1	Políticas y procedimientos de transferencia de información.	Se debe contar con políticas, procedimientos y controles de transferencias formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones
				A.13.2.3	Mensajería Electrónica.	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

Recursos

Humanos:

Especialista de seguridad de la información: Se requiere un Especialista en seguridad informática por un día aprox, para la redacción de la política. De acuerdo al mercado se puede asignar un valor por su consultoría de $50.000 por hora
Talento Humano: Una persona para revisión y redacción de la política.
Gerente General: Aprobación de la política para la seguridad de la información, aprobación de la compra del software de antivirus y aprobación del procedimiento de cifrado de la información crítica y secreta

Ingeniero de Sistemas: Se requiere de un Ing. de Sistemas para capacitar y monitorear la aplicación de las políticas y procedimientos. De acuerdo al mercado se puede asignar un valor mensual de $3.000.000
Abogado: Para revisión de la política y pertinencia legal.
Financieros:
Gerente financiero: Aprobación de disponibilidad presupuestal para la compra del software antivirus

Cuadro 26. (Continuación)

Acciones

Redactar la política respecto al control de acceso con base en lo requisitos del negocio y seguridad de la información.
Aprobación de la política por parte de la gerencia de INDUCON.
Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.
Cotizar, evaluar y adquirir e Implementar un software de antivirus empresarial para el control de virus.
Realizar seguimiento de los eventos que genere el aplicativo de software antivirus.
Capacitar a funcionarios de INDUCON en buenas prácticas para evitar contaminación y propagación de software malicioso.
Diseñar y documentar procedimientos para la transferencia de información.
Diseñar e implementar un procedimiento de cifrado de información crítica y secreta de INDUCON.
Aprobación por parte del Gerente General del procedimiento de cifrado.
Capacitación a los funcionarios de INDUCON, para el uso del proceso de cifrado de la información.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1	Especialista de seguridad de la información	01/09/2015	03/09/2015	Semestral	Especialista de seguridad de la información.
2	Gerente general	04/09/2015	04/09/2015	05/09/2015	Especialista de seguridad de la información.
3	Ingeniero de sistemas Talento Humano	15/09/2015	16/09/2015	18/09/2015	Especialista de seguridad de la información.
4	Ingeniero de sistemas	26/09/2015	Continua	Semestral	Especialista de seguridad de la información.
5	Especialista de seguridad de la información. Gerente General Compras	12/11/2014	19/11/2014	20/11/2014	Especialista de seguridad de la información.
6	Ingeniero de Sistemas	24/11/2014	Continuo	Mensual	Especialista de seguridad de la información.
7	Especialista de seguridad de la información.	26/11/2014	26/11/2014	Trimestral	Especialista de seguridad de la información.
Nro. Acción	**Responsable**	**Fecha Inicio**	**Fecha Fin**	**Fecha Seguimiento**	**Responsable de seguimiento**
8	Especialista de seguridad de la información.	30/09/2015	02/10/2015	Trimestral	Especialista de seguridad de la información
9	Especialista de seguridad de la información.	05/10/2015	07/10/2015	Continuo	Especialista de seguridad de la información.
10	Gerente General	8/10/2015	12/10/2015	13/10/2015	Especialista de seguridad de la información.
11	Especialista de seguridad de la información.	15/10/2015	15/10/2015	Continúo	Especialista de seguridad de la información.

Observaciones.

Fuente. Los Autores.

Cuadro 27. Plan de Tratamiento de los Riesgos Número 6, 7,11 y 14 Enunciados en el Cuadro 22.

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
6. 7. 11. 14.	Administración deficiente de los usuarios con acceso al sistema Abuso de privilegios. Administración deficiente de políticas de contraseña Principios de privilegios mínimos	A.9.1	Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
		A.9.4.	Evitar el acceso no autorizado a sistemas y aplicaciones.	A.9.4.1	Restricción de acceso a la información	El acceso a la información y las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
				A.9.4.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

Recursos

Humanos:

Especialista seguridad información: Se requiere de un Especialista en seguridad informática por dos días de para redacción de la política. De acuerdo al mercado, se puede considerar una asignación por su consultoría de $50.000 hora
Talento humano: Una persona para redacción y revisión de la política.
Gerente General: Para la aprobación de la política sobre control de acceso con base en los requisitos del negocio y de seguridad de la información.
Abogado: Persona jurídica para la revisión de condiciones y sanciones de la política.
Ingeniero de sistemas: Se requiere un Ing. de Sistemas por 30 días para la evaluación de las funciones de los sistemas de información. Adicional se requiere de otros dos días para implementar las políticas de contraseñas de aplicación y plataformas que la soportan (Sistema Operativo). De acuerdo al mercado, se considera un valor mensual de $3.000.000

Cuadro 27. (Continuación)

Acciones

Redactar la política respecto al control de acceso con base en lo requisitos del negocio y seguridad de la información.
Aprobación de la política por parte de la gerencia de INDUCON.
Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.
Realizar un plan de trabajo para la asignación de funciones en los aplicativos de acuerdo a la política de control de acceso.
Aprobación por parte de la Gerencia del plan de trabajo para la asignación de funciones.
Implementación controlada de las funciones en los aplicativos de acuerdo al plan de trabajo.
Monitorear la funcionalidad, registro de eventos y nuevas modificaciones.
Realizar planes de sensibilización a los funcionarios para el uso adecuado de las contraseñas y sus requisitos para su implementación.
Implementar el acceso de contraseñas en los servidores que soportan las aplicaciones con el fin de brindar accesos no autorizados a los sistemas de información.
Implementar el acceso de contraseñas en las aplicaciones que soportan la habilitación de políticas de contraseña.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	01/07/2015	03/07/2015	Semestral	Especialista de seguridad de la información.
2.	Gerente general	04/07/2015	04/07/2015	05/07/2015	Especialista de seguridad de la información.
3.	Talento humano	15/07/2015	16/07/2015	18/07/2015	Especialista de seguridad de la información.
4.	Especialista de seguridad de la información.	26/07/2015	Continua	Semestral	Especialista de seguridad de la información.|
5.	Administrador del sistema	01/08/2015	03/08/2015	Bimestral	Administrador del sistema
6.	Gerente General	04/08/2015	05/08/2015	06/08/2015	Administrador del sistema
7.	Ingeniero de sistemas	15/08/2015	15/10/2015	Bimestral	Administrador del sistema
8.	Ingeniero de sistemas	16/10/2015	Continua	Mensual	Administrador del sistema
9.	Talento Humano	17/10/2015	18/10/2015	Bimestral	Administrador Del sistema
10.	Ingeniero de sistemas	19/10/2015	19/10/2015	Semestral	Administrador del sistema
11.	Ingeniero de sistemas	20/10/2015	20/10/2015	Semestral	Administrador del sistema

Observaciones.

Fuente. Los Autores.

Cuadro 28. Plan de Tratamiento del Riesgo Número 8 Enunciado en el Cuadro 22

RIESGO		OBJETIVO DE CONTROL ISO 27001		CONTROL ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
8	Falta del manual de usuario para el manejo de la aplicación.	A.12.1	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.1	Procedimientos de operación documentados.	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.

Recursos

Humanos:
Ingeniero de Sistemas: se requiere de un Ing. de Sistemas para definir en los términos de referencia de los contratos que los proveedores de los sistemas de información deben cumplir entre otras obligaciones con la capacitación y entrega de manuales de usuarios actualizados de acuerdo a versiones y actualizaciones de los

Recursos

Sistemas. De acuerdo al mercado puede considerarse una asignación por un valor mensual de $3.000.000
Especialista en seguridad de la información: se requiere de un Especialista en seguridad informática para participar y aportar para la definición de los términos de referencia para la contratación de sistemas de información y tecnología de INDUCON. De acuerdo con el mercado se puede asignar un valor mensual de $3.500.000.

Abogado del área de contratación definir entre otras cláusulas los manuales de usuario y la capacitación como entregables durante el proceso de implementación de los sistemas de información.
Administrador de Sistemas: Capacitar a los usuarios finales en el uso de los manuales de usuario y en el manejo de los aplicativos.
Talento humano: Una persona para el manejo de inducción a nuevos funcionarios y a los que ya están en la organización.

Acciones

Definir en los términos de referencia de los contratos que los proveedores de los sistemas de información deben cumplir entre otras obligaciones con la capacitación y entrega de manuales de usuarios actualizados de acuerdo a versiones y actualizaciones de los sistemas.

Establecer una cláusula del contrato con los proveedores de los sistemas de información que los manuales de las aplicaciones, son documentos entregables durante el proceso de implementación del sistema y cuando haya actualización por nueva versión en los aplicativos.

Definir líneas de soporte al usuario final, cuando tenga inconvenientes con la funcionalidad del sistema.
Documentar los problemas e inconvenientes presentados a los usuarios finales respecto al uso del sistema, con el fin de tener una base de conocimiento de resolución de problemas.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información Ingeniero de Sistemas	04/01/2016	15/01/2016	Cuando se realicen contratos.	Especialista de seguridad de la información.
2.	Abogado área de contratación	18/01/2016	28/01/2016	Cuando se realicen contratos	Especialista de seguridad de la información.
3.	Ingeniero de Sistemas Administrador de sistemas	23/11/2015	27/11/2015	10/11/2015	Especialista de seguridad de la información.
4.	Administrador de sistema	09/11/2015	Continua	Mensual	Especialista de seguridad de la información Ingeniero de Sistemas.

Observaciones

Fuente. Los Autores.

Cuadro 29. Plan de Tratamiento de los Riesgos Número 9 Enunciado en el Cuadro 22

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
9.	Daño físico.	A.11.1	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2	Controles de acceso físico.	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.

Recursos

Humanos:

Especialista seguridad información: Se requiere de un Especialista en seguridad informática por dos días de para redacción del procedimiento para ingreso al centro de datos de INDUCON. De acuerdo al mercado. Perfil se puede asignar un valor por hora de consultoría de $50.000
Gerente General: Para la aprobación del procedimiento de seguridad de la información al ingreso al centro de datos.

Financiera: Disponer de presupuesto para la adquisición de una cámara adicional que está ubicada en el centro de datos para las operaciones que se realicen.

Acciones

Realizar un procedimiento de registro formal al centro de datos donde se registre, fecha ingreso, fecha salida, motivo del ingreso, empresa que ingresa o persona.

Proteger las áreas donde se encuentra información y recursos informáticos críticos de INDUCON mediante controles de acceso físico y seguridad ambiental.

Se debe definir en la política de seguridad de la información que está prohibido realizar actividades que pongan en peligro la integridad de los recursos informáticos de INDUCON tales como fumar, o el consumir alimentos y/o bebidas en las áreas donde estos residen.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	01/02/2016	03/02/2016	Semestral	Especialista de seguridad de la información.
2.	Ingeniero de sistemas	04/02/2016	11/02/2016	Bimestral	Ingeniero de sistemas
3.	Especialista de seguridad de la información	08/02/2016	08/02/2016	Semestral	Especialista de seguridad de la información.

Observaciones.

Fuente. Los Autores.

Cuadro 30. Plan de Tratamiento del Riesgo Número 10 Enunciado en el Cuadro 22.

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
10.	Daño lógico.	A.12.2	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra código maliciosos.	A.12.2.1	Controles contra código malicioso	Se deben implementar controles de detección, de prevención, y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
		A.12.5	Asegurarse de la integridad de los sistemas operacionales.	A.12.5.1	Instalación de software en sistemas operativos.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Recursos

Humanos:

Especialista seguridad información: Se requiere de un Especialista en seguridad informática por dos días de para redacción de la política. De acuerdo al mercado se considera un valor de $50.000 hora pos servicio de consultoría.

Gerente General: Para la aprobación del procedimiento de seguridad de la información al ingreso al centro de datos.

Talento humano: Una persona para redacción y revisión de la política.

Financiera: Disponer de presupuesto para la adquisición de una cámara adicional ubicada en el centro de datos para las operaciones que se realicen.

Abogado: Persona jurídica para la revisión de condiciones y sanciones de la política.
Ingeniero de sistemas: Se requiere de un Ing. de sistemas para la configuración y mantenimiento del aplicativo para la gestión de análisis de virus. De acuerdo al mercado se puede considerar un valor mensual de $3.000.000

Acciones

Redactar una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado.

Aprobación de la política por parte de la gerencia de INDUCON.

Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.

Cuadro 30. (Continuación)

Acciones

Redactar una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado.

Aprobación de la política por parte de la gerencia de INDUCON.

Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.

Implementación y actualización de herramienta de monitoreo de virus informático.

Implementación de reglas controladas de antivirus para la red entre esta están análisis de adjuntos, verificación de código en páginas web.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	10/02/2016	12/02/2016	Semestral	Especialista de seguridad de la información.
2.	Gerente general	15/02/2016	15/02/2016	16/02/2016	Especialista de seguridad de la información.
3.	Talento humano	17/02/2016	17/02/2016	18/02/2016	Especialista de seguridad de la información.
4.	Especialista de seguridad de la información.	19/02/2016	Continua	Semestral	Especialista de seguridad de la información.|
5.	Ingeniero de sistemas	11/15/2014	Continua	Bimestral	Ingeniero de sistemas
6.	Ingeniero de sistemas	22/02/2016	22/02/2016	Mensual	Ingeniero de sistemas

Observaciones:

Fuente. Los Autores.

Cuadro 31. Plan de Tratamiento del Riesgo Número 13 Enunciado en el Cuadro 22.

RIESGO		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
13.	Errores de mantenimiento / actualización de software.	A.12.1	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los
						Riesgos de acceso o cambios no autorizados al ambiente de operación.
		A.14.2	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.9	Prueba de aceptación de sistemas.	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
Recursos						
Humanos: Especialista seguridad información: Se requiere de un Especialista en seguridad informática para realizar procedimiento de control de versiones, gestión de actualizaciones, y gestión de errores. De acuerdo al mercado se puede considerar un valor mensual de $3.500.000 Ingeniero de sistemas: Se requiere de un Ing. de sistemas para configuración y mantenimiento base de datos pruebas, realizar separación de ambientes pruebas, producción. De acuerdo al mercado se puede considerar un valor de $3.000.000 valor mensual. Financiera: Evaluar presupuesto para la separación de ambiente de pruebas si es considerado en los planes de cambio por parte del Ingeniero de sistemas.					
Acciones						
Realizar un procedimiento que contemple el cambio de versiones de la aplicación donde se contemple la aceptación por parte de INDUCON. Implementar un procedimiento para instalaciones nuevas, actualizaciones y cambio de la aplicación. Se debe contar con una base de datos de pruebas actualizada con los últimos registros para realizar las diferentes pruebas y ejecución de comandos.						

Cuadro 31. (Continuación)

Acciones

Implementar ambientes separados de producción y pruebas para la aplicación core de INDUCON.
Se debe implementar un procedimiento para la gestión de errores.

Realizar un procedimiento donde se establezca los tipos de validación que se deben realizar antes de pasar a producción.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	24/02/2016	24/02/2016	Semestral	Especialista de seguridad de la información
2.	Especialista de seguridad de la información / Ingeniero de sistemas	25/02/2016	25/02/2016	26/02/2016	Especialista de seguridad de la información / Ingeniero de sistemas.
3.	Ingeniero de sistemas	29/02/2016	29/02/2016	Mensual	Ingeniero de sistemas
4.	Ingeniero de sistemas.	01/03/2016	15/03/2016	Bimestral	Ingeniero de sistemas
5.	Especialista de seguridad de la información / Ingeniero de sistemas.	16/03/2016	31/03/2015	Continuo	Ingeniero de sistemas
6.	Ingeniero de sistemas	01/04/2016	01/04/2016	Mensual	Ingeniero de sistemas

Observaciones:

Fuente. Los Autores.

Cuadro 32. Plan de Tratamiento del Riesgo Número 15 Enunciado en el Cuadro 22

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
15.	Errores de mantenimiento / actualización de software.	A.18.1	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2	Derecho de propiedad intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

Recursos

Humanos:

Especialista seguridad información: Se requiere de un Especialista en seguridad informática para realizar procedimiento de control de versiones, gestión de actualizaciones, y gestión de errores. De acuerdo al mercado se considera un valor de $3.500.000 mensual.

Ingeniero de sistemas: Se requiere de un Ing. de sistemas para configuración y mantenimiento base de datos pruebas, realizar separación de ambientes pruebas, producción. De acuerdo al mercado se considera una asignación de $3.000.000 mensual.

Financiera: Evaluar presupuesto para la separación de ambiente de pruebas si es considerado en los planes de cambio por parte del Ingeniero de sistemas.

Acciones

Realizar una política de cumplimiento de derechos de propiedad que defina el uso legal de software y cualquier otro producto informático.

Aprobación de la política por parte de la gerencia de INDUCON.
Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.

Monitorear la aplicación de la política.
Establecer un procedimiento para el área de compras donde se valide que el proveedor es confiable y no se violen derechos de autor en la adquisición de software o cualquier otro producto informático.

Se debe realizar un procedimiento para la gestión de activos de INDUCON referentes a tecnologías con el fin de proteger los derechos de propiedad intelectual.

Se debe contar con un espacio físico reservado bajo llave donde se almacene todo tipo de licencia física o medios.

Cuadro 32. (Continuación)

Acciones

Establecer un procedimiento para evaluar la cantidad de usuarios con que se cuenta la aplicación y el tipo de licenciamiento.

Realizar un procedimiento para realizar mantenimiento de software con el fin de establecer que solo existe software autorizado.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	04/04/2016	04/04/2016	Semestral	Especialista de seguridad de la información
2.	Gerente general	05/04/2016	06/04/2016	07/04/2016	Especialista de seguridad de la información
3.	Talento humano	12/04/2016	12/04/2016	13/04/2016	Especialista de seguridad de la información
4.	Ingeniero de sistemas	14/04/2016	Continua	Semestral	Ingeniero de sistemas
5.	Especialista de seguridad de la información / Ingeniero de sistemas	18/04/2016	18/04/2016	Continuo	Ingeniero de sistemas
6.	Ingeniero de sistemas	19/04/2016	19/04/2016	Mensual	Ingeniero de sistemas
7.	Ingeniero de sistemas	20/04/2016	20/04/2016	Mensual	Ingeniero de sistemas
8.	Ingeniero de sistemas	22/04/2016	22/04/2016	Mensual	Ingeniero de sistemas
9.	Ingeniero de sistemas	25/04/2016	25/04/2016	Mensual	Ingeniero de sistemas

Observaciones:

Fuente. Los Autores.

Cuadro 33. Plan de Tratamiento del Riesgo Número 16 Enunciado en el Cuadro 22

Riesgo		Objetivo de Control ISO 27001		Control ISO 27001		
Numero	**Descripción**	**Número**	**Descripción**	**Número**		**Descripción**
16.	No existe backup	A.12.3	Proteger contra la perdida de datos.	A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Recursos

Humanos:

Especialista seguridad información: Se requiere de un Especialista en seguridad informática para realizar procedimiento de control de versiones, gestión de actualizaciones, y gestión de errores. De acuerdo al mercado se considera una asignación de $3.500.000 mensual
Ingeniero de sistemas: Se requiere de un Ing. de sistemas para configuración y mantenimiento base de datos pruebas, realizar separación de ambientes pruebas, producción. De acuerdo al mercado se considera un valor de $3.000.000 mensual.
Financiera: Evaluar presupuesto para la separación de ambiente de pruebas si es considerado en los planes de cambio por parte del Ingeniero de sistemas.

Acciones

Realizar una política de copias de respaldo con los requisitos recomendados por la organización, debe contener los requisitos de retención y protección del backup.
Aprobación de la política por parte de la gerencia de INDUCON.
Capacitación y sensibilización para dar a conocer la política a todo nivel de la organización.
Monitorear la aplicación de la política.
Validar ubicación de almacenamiento de las copias de seguridad.
Establecer un procedimiento para el área de sistemas con la elaboración de las copias de respaldo que contemple documentación para recuperación y realización, frecuencia de las copias, protección física, poner a pruebas la recuperación del backup, si es información secreto empresarial deben estar cifradas.

Cronograma propuesto de implementación

Nro. Acción	Responsable	Fecha Inicio	Fecha Fin	Fecha Seguimiento	Responsable de seguimiento
1.	Especialista de seguridad de la información	27/04/2016	29/04/2016	Semestral	Especialista de seguridad de la información
2.	Gerente general	02/05/2016	02/05/2016	03/05/2016	Especialista de seguridad de la información
3.	Talento humano	05/05/2016	05/05/2016	06/05/2016	Especialista de seguridad de la información
4.	Ingeniero de sistemas	06/05/2016	Continua	Mensual	Ingeniero de sistemas
5.	Ingeniero de sistemas	10/05/2016	10/05/2016	Mensual	Ingeniero de sistemas
6.	Especialista de seguridad de la información / Ingeniero de sistemas	11/05/2016	13/05/2016	Bimestral	Ingeniero de sistemas

Observaciones:

Fuente. Los Autores.

5. CONCLUSIONES

Al finalizar el trabajo de investigación aplicada se logran los objetivos propuestos, de tal manera que el proyecto propuesto ha contribuido de manera positiva para el interés de INDUCON de mantener la seguridad de sus activos de información respecto a su confidencialidad, integridad y disponibilidad.

En el desarrollo del proyecto se logró identificar al interior del área de TI oportunidades de mejora respecto a la seguridad de la información, las cuales se evidenciaron mediante la realización del análisis del contexto interno como externo de la entidad, de la clasificación y valoración de los activos, del conocimiento del nivel de criticidad del activo respecto a su nivel de riesgo, el cual es determinado por las amenazas y vulnerabilidades a las cuales se encuentra expuesto el activo de información.

Igualmente, el proyecto proporciona con base en el análisis de riesgo de los activos de información, recomendaciones de medidas que llevadas a la implementación contribuirán a mitigar el riesgo de manera significativa, siempre teniendo como directriz de implementación el estándar de seguridad de la información ISO/27001:2013, la cual contiene los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información SGSI.

Durante el desarrollo del diseño del plan surgió la necesidad de implementar un control que permite a la empresa minimizar los riesgos asociados a la descarga de virus y gestionar los accesos por parte de los usuarios al contenido web como son páginas de videos, música y redes sociales, mejorando así el flujo de tráfico en la red, seguridad en las estaciones de trabajo, servidores de aplicación, base de datos y dominio, optimizando de mejor manera el banda ancha que cuenta la empresa permitiendo brindar mejor tráfico a los procesos core de INDUCON.

Para concluir, es importante resaltar que con el diseño del plan no se pretende garantizar la seguridad y protección total de los activos de información, sino llegar a minimizar el riesgo sobre estos a partir de la valoración de los mismos, el reconocimiento de los riesgos las amenazas y vulnerabilidades, logrando a si la disminución de la probabilidad de ocurrencia, como también de las consecuencias adversas que se generarían de llegar a desencadenarse un incidente de seguridad, es por ello que la formulación y posterior ejecución de medidas de seguridad permitirán a los empleados tener un mejor desempeño respecto al uso de los activos de información, proveyendo de esta misma manera a la herramientas las cuales le permitan hacer de la seguridad de la información no solo un sistema de gestión sino un estilo de vida.

.

6. RECOMENDACIONES

A continuación se presenta a INDUCON unas recomendaciones, con el fin de generar oportunidades que le permitan mejorar en aspectos referentes a la seguridad de la información.

- Es importante que INDUCON implemente políticas de calidad y un sistema de gestión de calidad, el cual le permitirá organizar e implementar el enfoque basado en procesos en la organización. La documentación de los procesos y el reconocimiento de estos por parte de la organización como documentos organizacionales bajo los cuales se rige un proceso o una determinada actividad, permitirá la mitigación de incidentes de seguridad de la información, ya que existiría un recurso físico bajo el cual los empleados podrían guiar su accionar respecto al proceso que esté vinculado.

- Es prioritaria y necesaria la formalización y divulgación de las políticas de seguridad de la información a todo nivel organizacional, con el fin qué esta sea adoptada por todos los funcionarios como una cultura institucional.

- Es importante para INDUCON, la definición y establecimiento de manuales de funciones por competencias. Igualmente, que a nivel interno cada área defina roles y responsabilidades a los funcionarios.

- Requiere un estudio técnico para definir debidamente el contexto externo de la entidad, con énfasis en definición de un modelo de estrategias competitivas en el mercado de la confección.

- El área de TI debe documentar los procesos para la transferencia de conocimiento y continuidad en las operaciones normales del área, en caso de ausencia de la persona responsable de las actividades.

- Se debe exigir a los proveedores de los diferentes sistemas de información, los manuales para usuarios finales alineados con los procesos para el uso adecuado de los aplicativos core del negocio.

- Es importante en INDUCON se realicen campañas de socialización y sensibilización de la importancia de la seguridad de la información dirigida a todo el personal administrativo y personal operativo.

BIBLIOGRAFÍA

ALMANZA, Andrés R. Encuesta. Seguridad informática en Colombia tendencias 2012-2013 [en línea]. Bogotá: Revista Sistemas [citado 10 marzo, 2015]. Disponible en Internet: <URL: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013>

CAMELO, Leonardo. Marco legal de Seguridad de la información [en línea]. Seguridad en Información en Colombia [citado 18 febrero, 2010]. Disponible en Internet: <URL: http://seguridadinformacionColombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html>.

CLADIRECT. Cuadrante Mágico 2013 de Gartner para Enterprise Network Firewalls [en línea]. Miami: La Empresa [citado 18 febrero, 2015]. Disponible en Internet: <URL: http://cladirect.com/2013/02/26/cuadrante-magico-2013-de-gartner-para-en terprise-network-firewalls/>

COMUNIDAD ANDINA. Decisión 486 de 2000 - Régimen Común sobre Propiedad Industrial [en línea]. Lima: La Comunidad [citado 18 febrero, 2015]. Disponible en Internet: <URL: www.comunidadandina.org/Sección.aspx?id...propiedad-intelectual>.

DE GERENCIA.COM. Análisis DOFA [en línea]. Bogotá: De Gerencia.com [citado 8 noviembre, 2011]. Disponible en Internet: <URL: http://www.degerencia.com/tema/analisis_dofa>

DINERO E IMAGEN. La importancia de implementar un plan de continuidad de negocio [en línea]. Bogotá: La Empresa [citado 1 julio, 2013]. Disponible en Internet: <URL: http://www.dineroenimagen.com/2013-07-01/22403>

EL PORTAL DE ISO 27001 EN ESPAÑOL. ISO 27000 SGSI Sistema de Gestión de Seguridad de la Información [en línea]. Bogotá: El Portal [citado 23 enero, 2015]. Disponible en Internet: <URL: http://www.iso27000.es/sgsi.html>.

GALLARDO, Sara. Cara y sello. Cultura de seguridad de la información, retos y cambios [en línea]. Bogotá: Revista Cultura de Seguridad de la Información, Retos y Cambios [citado 18 febrero, 2014]. Disponible en Internet: <URL: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no-127/item/131-cultura-de-seguridad-de-la-informaci%C3%B3n-retos-y-cambios>

GARTNER. Matriz de amenazas y vulnerabilidad (motor de base de datos) [en línea]. Bogotá: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL: https://technet.microsoft.com/es-es/library/bb895180(v=sql.105).aspx>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001. Bogotá: ICONTEC, 2013. 45 p.

-------. Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. 11 p.

INSTITUTO NACIONAL DE CIBER SEGURIDAD – INCIBE. Ciberseguridad [en línea]. Madrid: El Instituto [citado 18 febrero, 2010]. Disponible en Internet: <URL: https://www.incibe.es/>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO. ISO International Standards [en línea]. Ginebra: ISO [citado 23 enero, 2015]. Disponible en Internet: <http://www.iso.org/iso/home/standards.htm>

MAGERIT. Entorno del análisis de riesgos [en línea]. Madrid: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL: https://www.ccn-cert.cni.es/ publico/herramientas/pilar5/ magerit/>

PORTER, Michael E. Modelo de las cinco fuerzas de Porter [en línea]. Bogotá: Wikipedia [citado 18 febrero, 2015]. Disponible en Internet: <URL: es.wikipedia.org/wiki/Análisis_ Porter_de_las_cinco_fuerzas>.

SEGURIDAD EN INFORMACIÓN EN COLOMBIA. Marco legal de Seguridad de la información [en línea]. Bogotá: Blogspot [citado 18 febrero, 2010]. Disponible en Internet: <URL: http://seguridadinformacionColombia.blogspot.com/2010/02/seguir dad-de-la-informacion-y-seguridad.html>

TECHNET. Vulnerabilidades de motor de base de datos [en línea]. Madrid: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL: https://technet. microsoft.com/es-es/library/ bb895180(v=sql.105).aspx>

--------. Matriz de amenazas y vulnerabilidad motor de base de datos [en línea]. Madrid: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL: https://technet.microsoft. com/ es-es/librar/bb895180(v=sql.105).aspx>

WIKIPEDIA. La seguridad informática [en línea]. Bogotá: Wikipedia [citado 18 febrero, 2010]. Disponible en Internet: < http://es.wikipedia.org/wiki/Seguridad_ informática>

-------. Diseño asistido por computadora [en línea]. Bogotá: Wikipedia [citado 23 enero, 2015]. Disponible en Internet: <URL: https://es.wikipedia.org/wiki/CAD/ CAM>.

-------. Fabricación asistida por computadora [en línea]. Bogotá: Wikipedia [citado 23 enero, 2015]. Disponible en Internet: https://es.wikipedia.org/wiki/ CAD/CAM>

ANEXOS

Anexo A. Encuesta Seguridad de la Información en INDUCON

ENCUESTA SEGURIDAD INFORMÁTICA INDUCON

La siguiente encuesta tiene como finalidad validar el estado actual de la seguridad de la información en INDUCON.
Marque con una X la opción correspondiente

Nombre completo: _____ Área: _____

- ¿Conoce usted que es una política de seguridad de la información?
  SI NO

- ¿Cuándo usted ingreso a INDUCON le informaron las políticas de seguridad de la información?
  SI NO

- ¿Al realizar contratos con empresas externas exigen alguna clausula referente a seguridad de la información?
  SI NO

- ¿Cuando ocurre un incidente de seguridad de información usted lo reporta? ¿A quién?
  SI NO _____

- ¿Conoce alguna política de confidencialidad de la información en INDUCON?
  SI NO

- ¿Las áreas de la empresa están identificadas claramente?
  SI NO

- ¿Qué mecanismo de control tiene la empresa para el ingreso a la oficina donde usted desempeña sus funciones?
  Cual _____

- ¿En caso de alguna falla en la red están preparados para continuar con la operación?
  SI NO

- ¿Si se presenta algún daño en el equipo tiene como continuar la operación?
  SI NO

- ¿Sabe si su equipo cuenta con herramientas para análisis de virus?
  SI NO

- ¿Usted cuenta con una clave para ingresar al computador cuando lo enciende?
  SI NO

- ¿Cuenta con alguna clave para acceder a los aplicativos?
  SI NO

- ¿Tiene algún problema con el computador actualmente?
  SI NO

- ¿Usted tiene claro el procedimiento y a quién debe reportar cuándo tiene problemas con su computador o con los sistemas que maneja?
  SI NO ¿A QUIEN? _____

- ¿El tiempo de respuesta ante un incidente informático es el adecuado?
  TOTALMENTE DE ACUERDO ___
  DE ACUERDO ___
  MEDIANAMENTE DE ACUERDO ___
  EN DESACUERDO ___

- ¿Considera importante el apoyo de las TI para el cumplimiento de los objetivos estratégicos de INDUCON?
  SI NO

- ¿Considera que maneja información que es considerada secreto empresarial? "Cualquier información no divulgada que legítimamente posea para sus actividades productivas".
  SI NO

- ¿Considera que su información debe estar respaldada por un Backup?
  SI NO

- ¿Cuándo usted ingresó a la empresa recibió capacitación o inducción respecto a seguridad de la información y a los sistemas que iba a manejar?
  SI NO

- ¿Cuándo una persona se pensiona o renuncia a la empresa es inactivado para el acceso al sistema?
  SI NO

- ¿Qué área le asignó el usuario y la clave para el acceso a los sistemas de información? ¿Cuál? _____

- ¿Usted puede copiar información del computador a una USB, CD, DVD o cualquier otro medio extraíble?
  SI NO

- ¿Usted realiza copias de seguridad de la información de su computador?
  SI NO

- ¿En el momento de retirarse del puesto de trabajo deja bloqueado el acceso a su computador?
  SI NO

Anexo B. Encuesta Seguridad de la Información en el Área de TI.

ENCUESTA SEGURIDAD INFORMÁTICA INDUCON

La siguiente encuesta tiene como finalidad validar el estado actual de la seguridad de la información en INDUCON en el área de TI.

Marque con una X la opción correspondiente

Nombre completo: _____ Área: _____

- ¿Conoce usted que es una política de seguridad de la información?
  SI NO

- ¿Conoce de alguna política para el uso adecuado de dispositivos móviles en INDUCON?
  SI NO

- ¿Existe algún proceso disciplinario con el fin de emprender acciones contra empleados que hayan cometido alguna violación a la seguridad de la información en INDUCON?
  SI NO

- ¿Se cuenta con un listado de activos de información?
  SI NO

- ¿Existe algún procedimiento para la disposición de medios cuando ya no son requeridos por la empresa?
  SI NO

- ¿Existe algún control para especificar el uso adecuado de servicios de red o recursos compartidos?
  SI NO

- ¿Existe un procedimiento formal para la cancelación y registro de usuarios para asignar accesos?
  SI NO

- ¿Existe algún proceso para sensibilizar a los usuarios de usar adecuadamente la autenticación en los sistemas de información?
  SI NO

- ¿Se valida correctamente el uso adecuado de gestión de contraseñas en las aplicaciones?
  SI NO

- ¿Las áreas consideradas seguras cuenta con algún control fisco de acceso?
  SI NO

- ¿Se cuenta con un sistema de UPS para proteger los servidores en una caída de energía?
  SI NO

- ¿Se cuenta con ambientes separados para realizar pruebas de la aplicación?
  SI NO

- ¿Los Backups que se realizan al sistema de información son probados frecuentemente?
  SI NO

- ¿Existe un control para llevar un registro de incidentes, eventos de seguridad de la información?
  SI NO

- ¿Existen procedimientos para la instalación de software en los equipos cliente y servidor?
  SI NO

- ¿La red de INDUCON esta segmentada por áreas de negocio?
  SI NO

- ¿Se lleva a cabo un procedimiento de revisión técnica de la aplicación crítica del negocio después de algún cambio?
  SI NO

- ¿Existe procedimientos que permitan la continuidad de negocio con la aplicación core de INDUCON?
  SI NO

- ¿Se maneja un control de licenciamiento para cumplir con los derechos de autor?
  SI NO

- ¿Se da cumplimiento a la protección y privacidad de la información de datos personales de los usuarios del sistema de información?
  SI NO

- ¿Existen procedimientos para el uso aceptable de los sistemas de información?
  SI NO

- ¿El cableado de comunicaciones está protegido contra interceptación, daño?
  SINO

- ¿Se realiza un mantenimiento preventivo y correctivo de los equipos de cómputo?
  SI NO

- ¿Existen procedimientos formales que ayuden a validar la transferencia de información para protegerla?
  SI NO

- ¿Existe a nivel de TI un marco de trabajo para la administración del riesgo de TI?
  SI NO
- ¿Existe un plan de seguridad de TI en la organización?
  SI NO

- ¿Se cuenta con procedimientos para la administración de cuentas de usuario, que contemple: la solicitud, el establecimiento, la emisión, modificación y cierre de cuentas de usuario y de los privilegios relacionados?
  SI NO

- ¿Durante el ciclo de planeación, se plantean interrogantes a las áreas usuarias sobre sus necesidades de recursos informáticos?
  SI NO

- ¿Se controla y protege en forma regular la integridad y consistencia de los datos?
  SI NO

- ¿Están protegidos contra robo o uso no autorizado los archivos que contienen los programas de la compañía: copias de las bases de datos periódicamente, Existen controles para verificar que se usan las versiones correctas de los archivos en el procesamiento?
  SI NO

Anexo C. Listado Completo de Amenazas

Activo	Amenazas
Servidor de aplicaciones y base de datos.	• Daño físico. • Daño lógico. • Software malicioso. • Mal funcionamiento del software. • Uso no autorizado del equipo. • Espionaje remoto. • Eventos naturales. • Susceptibilidad a las variaciones de voltaje. • Susceptibilidad a las variaciones de temperatura.
Servidor de dominio.	• Daño Físico. • Falla suministro de energía. • Falla técnica. • Mal funcionamiento del equipo. • Software malicioso. • Daño lógico. • Eventos naturales. • Actualización sin supervisión.
Estaciones de trabajo de los usuarios.	• Daño físico. • Daño lógico. • Mal funcionamiento del software. • Malware. • Mal funcionamiento por falta de actualización de parches. • Hurto. • Errores de mantenimiento / actualización de equipos. • Escritorio desatendido.
Planta telefónica.	• Daño físico. • Mal funcionamiento.
Impresoras.	• Daño físico. • Mal funcionamiento. • Obsolescencia. • Interrupción de otros servicios y suministros esenciales. (Falta de tóner).
Medios para datos.	• Daño físico. • Daño lógico.
Software	
SAP Business One.	• Errores de los usuarios (Equivocaciones de las personas en la captura de datos). • Errores de mantenimiento / actualización de programas. • Mala aplicación de un parche. • Falta del manual de usuario para el manejo de la aplicación. • Errores del administrador. • Errores de configuración. • Defectos en el código de los programas. • Caída del sistema por agotamiento de recursos. • Abuso de privilegios.

Anexo C. (Continuación)

Activo	Amenazas
SAP Business One.	• Administración deficiente de los usuarios con acceso al sistema.
Modaris.	• Errores de los usuarios (Equivocaciones de las personas en la captura de datos). • Mala aplicación de un parche. • Errores de configuración. • Caída del sistema por agotamiento de recursos.
Diamino.	• Errores de los usuarios (Equivocaciones de las personas en la captura de datos). • Errores de mantenimiento / actualización de programas. • Caída del sistema por agotamiento de recursos.
Helisa SGW.	• Errores de mantenimiento / actualización de programas. • Administración deficiente de los usuarios con acceso al sistema.
Willcom.	• Falta de monitorización por estar instalado en la estación del usuario que lo maneja. • Manipulación con software.
Stym.	• Obsolescencia en las herramientas de desarrollo. • Mala aplicación de un parche. • Errores de configuración. • Administración deficiente de políticas de contraseña. • Administración deficiente de los usuarios con acceso al sistema.
Corel Draw 7.0.	• Errores de mantenimiento / actualización de programas.
Sistema operativo server.	• Errores de mantenimiento / actualización de software. • Espionaje remoto. • Malware (Virus, spyware). • Avería de origen físico / lógico. • Errores de monitorización (log). • Caída del sistema por agotamiento de recursos. • Administración deficiente de los usuarios con acceso al sistema. • Administración deficiente de políticas de contraseña.
Sistema operativo cliente.	• Errores de mantenimiento / actualización de software. • Espionaje remoto. • Malware (Virus, spyware). • Avería de origen físico / lógico. • Manipulación errónea de la configuración del equipo.
Software de ofimática.	• Errores de mantenimiento / actualización de software. • Software no licenciado. • Error de usuario (borrado de archivos).
Software de Base de datos SQL.	• Errores de mantenimiento / actualización de software.

Anexo C. (Continuación)

Activo	Amenazas
Software de base de datos SQL.	• Mala gestión de directivas de seguridad. • Principios de privilegios mínimos(*). • Validación de boletines de seguridad(**) • Validación de los puertos de red(***). • Configuración incorrecta de las cuentas de servicio.
Software colaborativo.	• Errores de mantenimiento / actualización de software. • Principio de privilegios mínimos. • Administración deficiente de los usuarios con acceso al sistema. • Validación de puertos de la aplicación(****).
Correo empresarial.	• Uso inadecuado del correo. • Descarga de contenido como virus, gusanos y todo clase malware. • Demora en la atención de solicitudes por falla en la plataforma.
Personal	
Administrador de base de datos.	• Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. • Uso inadecuado de procedimientos en la base de datos.
Soporte nivel 1 ofimática, hardware.	• Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. • Daño físico por desconocimiento. • Daño lógico por desconocimiento.
Soporte aplicaciones.	• Conocimiento insuficiente del funcionamiento de la aplicación. • Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. • No definición de roles.
Mesa de ayuda.	• Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.
Administrador de red.	• Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. • Falta de conocimiento en la integración de redes. • Falta de monitorización de los registros de log de los dispositivos de red. • No definición de roles.
Administrador de seguridad.	• Indisponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público. • Error en el uso.
Administrador de seguridad.	• Realizar pruebas en ambientes de producción. • Uso excesivo de restricciones para el uso del sistema. • No definición de roles.
Red.	

(*)Principio de privilegios mínimos un sistema solo debería permitir un nivel de acceso necesario a un objeto protegible y debe estar habilitado para los que tienen una necesidad directa y solo por un tiempo específico.
(**)Boletines de seguridad se deben validar los boletines de seguridad que son emitidos por las entidades donde ya fueron probados y validados con el fin de no poner en peligro al sistema por no implementarlo
(***)Validación puertos de red, puertos estándar están abiertos a internet se puede presentar un ataque
(****)Validación puertos de red, puertos estándar están abiertos a internet se puede presentar un ataque.

Anexo C. (Continuación)

Activo	Amenazas
Centro de datos.	• Fuego. • Falla en el suministro de energía. • Refrigeración. • Falla del equipo de comunicaciones. • Espionaje remoto.
Equipos activos de red.	• Falta de configuración de bloqueo de puertos. • Daño físico. • Daño lógico • Mal funcionamiento del equipo. • Falla en el suministro de energía. • Desgaste.
Planta telefónica.	• Daño físico. • Daño lógico. • Mal funcionamiento del equipo.
Modem ISP.	• Daño físico. • Caída del servicio. • Desprotección en la puerta de enlace.
Routers inalámbricos.	• Daño físico. • Daño lógico. • Interferencia de señal. • Mala configuración del dispositivo.

Fuente. Los Autores.

DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA COMPAÑÍA INDUCON UBICADA EN BOGOTÁ

Ana Cecilia Castrillón Barreto, Juan Pablo Falla Sánchez

***Abstract*— To carry out the design of a plan of information security for the area of IT Inducon, fieldwork was conducted, conducting interviews, surveys at different levels of the organization and analysis of internal and external context, highlighting needs and security expectations. According to the above, and based on the guidelines of the ISO 27001: 2013 and 27005: 2009 were identified, categorized and criteria for the treatment of risks were defined, identified and evaluated assets under the criteria of confidentiality, integrity and availability, threats and vulnerabilities were identified. Finally, we proceed to make the risk matrix for each asset and risk treatment plan based on control objectives of ISO 27001: 2013. Since the objective of the organization is to prepare the medium term for the formal implementation of an ISMS and because it is their first experience with management systems and lacks the resources to cope with a full implementation of the ISMS, it will be delivered as an end result the document Plan information security for the IT**

***Index Terms*—Informática, información, integridad, disponibilidad, confidencialidad, riesgo, amenaza y vulnerabilidades.**

I. INTRODUCTION

En la época de la sociedad del conocimiento en la que se desarrolla el mundo actual, las empresas requieren basar sus procesos en sistemas informáticos que cada día dependen más de nuevas tecnologías, las cuales vienen acompañadas de riesgos en el manejo de la información, por lo tanto, éstas requieren adecuada administración partiendo de la identificación de los elementos críticos y sobre todo tener identificados y clasificados los riesgos, las amenazas y las vulnerabilidades, para luego diseñar estrategias y controles apropiados de mitigación en cuanto a su protección y seguridad.

Por lo tanto, es necesario que las empresas dediquen esfuerzo, tiempo y recursos para la protección de su infraestructura de tecnologías de la información y las comunicaciones y de su activo más valioso como es la información; es por esta razón, que al revisar el tema de gobierno de TI en la empresa INDUCON de Colombia se evidencia la necesidad de realizar el diseño de un plan de seguridad de la información, para el área de TI de la compañía, cuyo objetivo de negocio es el diseño, corte y confección de dotaciones industriales y prendas militares.

Una vez terminado el trabajo de investigación aplicada se suministrará a INDUCON el diseño de un plan de seguridad de la información, para los procesos críticos del área de TI, mapa de riesgos, concientizar, capacitar y lograr en conjunto con la alta gerencia de INDUCON la definición y aprobación de una política de seguridad de la información, con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información.

II. PROBLEMA

Se realizó un análisis de la situación actual de INDUCON, la cual cuenta con bastantes recursos tecnológicos, humanos e infraestructura que apoyan la operación, sin embargo se evidencia la falta de procedimientos, políticas para el uso adecuado de los recursos tecnológicos, mapa de riesgos, un plan de seguridad de la información para garantizar la confidencialidad, disponibilidad e integridad de la información, por eso se hace necesario de ¿cómo crear el diseño de un plan de seguridad de la información para el área de TI?.

III. MARCO TEÓRICO

El plan de seguridad de informática para un área de TI comprende las políticas, estructura organizativa, procedimientos, procesos y recursos necesarios para implementar la gestión de seguridad de la información, de este modo se utiliza de acuerdo al estándar de seguridad la norma ISO 27001, la cual se basa en buenas prácticas y objetivos de control establecidos en la ISO 27002. El fundamento de esta norma se centra en la confidencialidad, integridad y disponibilidad mediante la aplicación de un proceso de gestión del riesgo. Por lo anterior, resulta imprescindible que las

entidades identifiquen los riesgos que pueden afectar su información y sus activos, de manera que se pueda crear un plan para tratar apropiadamente los riesgos.

Como lo define la norma ISO 27001, "la adopción de un SGSI es una decisión estratégica para la organización y el establecimiento e implementación del SGSI tienen influencia en las necesidades y objetivos de ésta, los requisitos de seguridad, los procesos organizacionales empleados, el tamaño y estructura de la organización". El establecimiento del SGSI incluye definir cuál será el alcance, límites y por tanto la política de seguridad de la información, para luego implementar y operar el SGSI, diseñar y ejecutar procedimientos de seguimiento, revisión y otros controles que permitan definir después cuáles serán las acciones de mantenimiento y mejora.

A. Contexto Interno.

Industrias y Confecciones INDUCON SAS, es una empresa del sector de fabricación, dedicada a la confección de dotaciones industriales con la mejor calidad, especializada en confección de ropa y accesorios para protección personal, identificación corporativa uniformes y prendas militares. Entre sus clientes se encuentran: Alpina, Carrefour, Avianca, Pavco, Zenú, Meals de Colombia S.A., Ministerio de Minas y Energía, Ministerio de Defensa Nacional entre otros.

INDUCON, nace en abril 28 de 1984, como el desarrollo de una idea de negocio de su fundador. Como todo lo que se construye con esfuerzo y dedicación, INDUCON ha logrado tomar forma y abrirse un espacio importante dentro del gremio de las confecciones, ubicándose como una de las empresas de mayor reconocimiento en el campo de las dotaciones industriales y prendas militares a nivel nacional e internacional, incorporando a su infraestructura la mejor mano de obra, y lo último en CAD (tecnología de diseño asistido por computador), corte y confección, actualmente cuenta con aproximadamente 250 trabajadores, dentro de los cuales se destacan profesionales en diseño de modas, técnicos expertos en el manejo de tecnología de corte CAM (fabricación asistida por computador), personal experto y calificado en corte y confección, expertos en control de calidad, operarios entre otros.

Para INDUCON un uniforme es una prenda que traduce una imagen adecuada, es la apariencia visible de una persona o profesión, lo que se proyecta a la sociedad y esta a su vez percibe de quien la viste, un uniforme traduce el compromiso, el amor y la identidad profesional, proyecta la capacidad de impartir justicia, dar y recibir respeto, asumir responsabilidad, brindar comprensión, esperanza, tolerancia y prudencia. Para realizar el contexto interno y externo de INDUCON, se tuvo en cuenta la plataforma estratégica, la estructura orgánica, la infraestructura tecnológica y se realizó el modelo de la cadena de valor y el modelo de las cinco fuerzas de Porter las cuales son: rivalidad entre competidores, amenaza de los nuevos competidores, amenaza de productos y servicios sustitutos, poder de negociación de los proveedores y clientes.

B. Contexto Externo.

Confecciones INDUCON, es consciente que el proceso de globalización es imposible de ignorar y que por lo tanto, debe aplicar estrategias para estar a la vanguardia en el sector de la confección. La empresa está decidida a implementar un proceso de mejoramiento continuo, encaminado a la búsqueda del control de los procesos, definición de políticas de calidad y de seguridad de la información y definir determinados planes como el de este proyecto.

Igualmente, INDUCON tiene presente el modelo de análisis de la competencia de las cinco fuerzas de Michael Porter, el cual es utilizado por muchas industrias como instrumento de gestión para la elaboración de estrategias tomando en cuenta el entorno externo.

Tomando como base el modelo de Porter, se realizó con el área de mercadeo un análisis estratégico haciendo referencia a la posición actual de la compañía y su entorno competitivo internacional, se validó el ambiente nacional, el cual busca determinar el contexto donde opera la compañía, sus ventajas competitivas en el mercado mundial y un factor importante, es la parte legal y tecnológica, que pueden en un momento dado afectar la organización.

Una de las amenazas que enfrenta INDUCON, es la competencia, se sabe que entre mayor competencia, menor fuerza y por consiguiente el riesgo es más alto y las utilidades también se reducen de una manera proporcional.

C. Necesidades y expectativas en seguridad de la información.

Para determinar las necesidades y expectativas en materia de seguridad de la información de las partes interesadas, se procedió a realizar entrevistas, encuestas a los diferentes funcionarios, de los cuales surge la necesidad de implementar un plan de seguridad para el área de TI, capacitaciones sobre seguridad informática, que existan políticas del uso de las tecnologías de comunicación, planes de contingencia de los sistemas de información. Con respeto a las expectativas se espera continuidad del funcionamiento de los sistemas, solución pronta a contingencias, se realicen de manera eficiente los planes de Backup, se estandaricen los procesos y se realicen capacitaciones en seguridad de la información.

D. Alcance del sistema de gestión de la seguridad de la información.

El alcance del presente proyecto es el diseño del plan de seguridad de la información para el área de TI en INDUCON ubicado en la ciudad de Bogotá, basados en el contexto interno y externo de la organización, en la identificación de necesidades y un análisis de riesgos; con el fin de

proporcionarle una herramienta que le permitirá en un futuro la implementación de un SGSI para el área de TI.

IV. RIESGOS

Para la elaboración del análisis de riesgos se utilizó la Norma Técnica Colombiana NTC-ISO/IEC 27005:2009, estableciendo el contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo. (Véase Figura I).

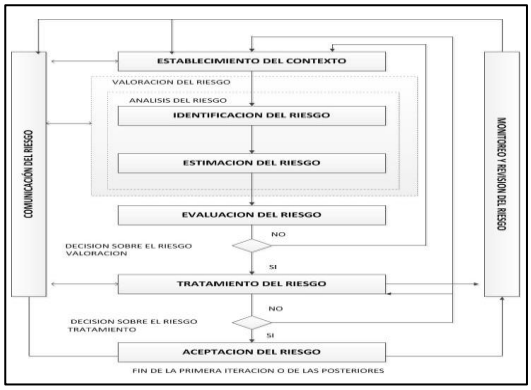


Figura I: Metodología del riesgo.

Fuente. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO/IEC 27005. Bogotá: ICONTEC, 2009. p.5Equations.

Para la categorización del riesgo se tomaron factores como económico, humanos, legales, tecnológicos y naturales, se definieron las tablas de probabilidad, impacto se cruzaron y multiplicaron para determinar la escala de tratamiento del riesgo, posteriormente se validaron los resultados del análisis del riesgo y se preparó un plan para su tratamiento. Algunos de los riesgos críticos identificados fueron: daño físico y lógico de los servidores que soportan las aplicaciones y base de datos, administración deficiente de los usuarios con acceso al sistema, deficiencia en la asignación de contraseñas, errores de mantenimiento y actualización de software.

V. IDENTIFICACIÓN DE ACTIVOS

En el área de TI de INDUCON se soportan diferentes servicios, y con base al levantamiento de información de la infraestructura tecnológica, se procedió a identificar los diferentes activos agrupados en hardware, software, red, personal e instalaciones (Véase el cuadro I), se procedió a valorar cada activo, bajo los criterios de disponibilidad, confidencialidad e integridad, a estos activos se les identifico las amenazas que son críticas para cada uno de ellos con el fin de mitigar el impacto de ocurrencia en los activos, apoyados con la norma técnica NTC-ISO/IEC Colombiana 27005:2009, y la experiencia profesional de los integrantes de este proyecto, posteriormente se identificaron las vulnerabilidades a las cuales están sometidos los activos, utilizando un modelo de alto nivel donde se abordó un enfoque global de la organización.

CUADRO I
IDENTIFICACIÓN DE ACTIVOS

Hardware	**Descripción**
Servidor de aplicaciones y base de datos	Soporta las aplicaciones de SAP Business One, Helisa SGW, Motor base de datos SQL Server 2008.
Servidor de dominio	Soporta el Directorio Activo, recursos compartidos para Modaris, Diamino (aplicativos de diseño).
Estaciones de trabajo de los usuarios	Soporta software ofimático, correo corporativo, aplicación cliente de SAP
Planta telefónica	Comunicación telefónica
Impresoras	Impresión documentos
Medios para datos	Medios de almacenamiento de datos
Software:	**Descripción**
SAP Business One	ERP compuesto por 8 módulos
Modaris	Software de patronaje
Diamino	Software para crear marcadas y colocar las piezas
Helisa SGW	Software contable
Willcom	Software para la realización de bordado
Stym	Métodos y tiempos para producción
Corel Draw 7.0	Aplicativo para diseñar el modelo o la prenda
Sistema Operativo Server	Software que soporta las aplicaciones servidor
Sistema Operativo Cliente	Software que soporta las aplicaciones cliente
Software de ofimática	Software que soporta las actividades diarias.
Software de Base de datos SQL	Soporta los datos de la aplicación SAP
Software colaborativo	Herramienta colaborativa para centralizar las comunicaciones
Correo empresarial	Herramienta de gestión de correos
Red:	**Descripción**
Centro de datos	Alojamiento de equipos activos de red y comunicaciones.
Equipos activos de red	Soportan la comunicación interna y externa de INDUCON
Planta telefónica	Comunicación telefónica
Modem ISP	Router del proveedor del servicio
Routers inalámbricos	Señal inalámbrica
Personal:	**Descripción**
Jefes de oficinas	Personas que toman decisiones
Usuarios	Usuarios de las diferentes aplicaciones
Personal de operación/ mantenimiento	Administración y control de las aplicaciones, copias de seguridad, mesa de ayuda.
Instalaciones:	Descripción
Centro de cómputo	Acceso controlado para el ingreso mediante seguro de puerta.

Fuente: Autores

A. *Resumen de activos a tratar.*

La valoración de los activos es necesario realizarla en función de la relevancia que estos tengan para la empresa y del impacto que una incidencia sobre el mismo pueda causar a la entidad y que afecte la confidencialidad, integridad y disponibilidad. En el (cuadro II) se relacionan los activos de TI, que arrojaron un impacto alto de riesgo, por lo tanto deben ser tratados. El impacto alto está definido por la sumatoria de la confidencialidad, integridad y disponibilidad.

CUADRO II
IDENTIFICACIÓN DE ACTIVOS

Activo	Descripción	C	I	D	Σ
Servidor de aplicaciones y base de datos.	Soporta las aplicaciones de SAP Business One, Helisa SGW, Motor base de datos SQL Server 2008.	3	3	3	9
Software de Base de datos SQL.	Soporta los datos de la aplicación SAP.	3	3	3	9
SAP Business One.	ERP compuesto por 8 módulos.	3	3	3	9
Sistema operativo server.	Software que soporta las aplicaciones servidor.	3	3	3	9
Administrador de base de datos.	Responsable de la administración, control y monitoreo de la base de datos.	3	3	2	8
Medios para datos.	Medios de almacenamiento de datos.	2	3	3	8
Servidor de dominio.	Soporta el Directorio Activo, recursos compartidos para Modaris, Diamino (aplicativos de diseño).	3	2	3	8
Stym.	Métodos y tiempos para producción.	2	3	3	8
Soporte aplicaciones.	Responsable de soporte a usuario final.	3	2	3	8
Administrador de la seguridad.	Responsable de la seguridad de la información.	3	2	3	8
Helisa SGW.	Software contable.	2	3	2	7
Sistema operativo cliente.	Software que soporta las aplicaciones cliente.	3	3	1	7
Software de ofimática.	Software que soporta las actividades diarias.	3	3	1	7
Administrador de red.	Responsable del funcionamiento de la arquitectura de red.	2	2	2	6
Modaris.	Software de patronaje.	1	3	2	6
Diamino.	Software para crear marcadas y colocar las piezas.	1	3	2	6
Willcom.	Software para la realización de bordado.	1	3	2	6
Corel Draw 7.0.	Aplicativo para diseñar el modelo o la prenda.	1	3	1	5
Software colaborativo.	Herramienta colaborativa para centralizar las comunicaciones.	3	1	1	5
Correo empresarial.	Herramienta de gestión de correos.	3	1	1	5

Fuente: Autores

VI. IDENTIFICACIÓN DE AMENAZAS

Una vez identificado los activos en los cuales el valor es más alto de acuerdo con su confidencialidad, integridad y disponibilidad, se identifican las amenazas que son críticas para cada uno de ellos, con el fin de mitigar el impacto de ocurrencia en los activos.

Para la identificación de las amenazas se utilizó la información obtenida en las entrevistas y encuestas realizadas a los funcionarios de los diferentes niveles de INDUCON, apoyados en la norma técnica NTC-ISO/IEC Colombiana 27005 y la experiencia profesional de los realizadores de este proyecto.

VII. IDENTIFICACIÓN DE VULNERABILIDADES

Para identificar las vulnerabilidades se utiliza un modelo de alto nivel que permite abordar una visión más global de la organización y su sistema de información, tomando como punto de referencia el análisis del contexto interno y externo de INDUCON concentrándonos más en el negocio, y determinando así los activos más relevantes.

Se procede a identificar un listado de amenazas y vulnerabilidades para cada activo de la organización y nos centramos en validar los más críticos, agrupados en un dominio y finalmente seleccionar los objetivos de control específicos que ayuden a mitigar esos riesgos, buscando un enfoque sencillo que facilite la aceptación de un plan de trabajo para la valoración de riesgos, minimizar los recursos económicos, y aplicarlos donde así se consideren necesarios y se obtenga un mayor beneficio en la necesidad de protección.

Se evidencia que la mayoría de vulnerabilidades son por la ausencia de procedimientos para la gestión adecuada de TI, la falta de concientización en seguridad de la información, el uso inadecuado de los sistemas de información, la falta de capacitación en temas de seguridad como también una correcta definición de roles y responsabilidades. Sin descuidar que los recursos tecnológicos como son el hardware y software son fundamentales y toman un papel importante en las actividades que se realizan día a día en la empresa.

Todas estas vulnerabilidades deben ser tratadas y minimizadas con el fin de ayudar a INDUCON a mitigar los riesgos.

VIII. MATRIZ DE RIESGO

Una vez definidos los activos, valorados sus riesgos frente a los criterios definidos se procede a realizar la matriz de riesgos, donde se define el activo, el riesgo asociado y se genera el nivel del riesgo al cual están expuestos los activos, valorando la probabilidad por el impacto para cada uno de los activos, el resultado del nivel es calculado tomando la escala de la probabilidad para cada riesgo que se obtiene de la multiplicación de la probabilidad de ocurrencia de un evento por el impacto.

Para determinar los valores de la escala de probabilidad fue necesario realizar una entrevista con el Ingeniero de sistemas de la empresa, evaluando cada uno de los riesgos asociados, su frecuencia y probabilidad de ocurrencia de la misma, la escala toma unos valores de 1 a 5 siendo uno (1) muy bajo; donde el incidente puede ocurrir en una circunstancia excepcional, en cambio el calificativo de cinco (5) se espera que el incidente ocurra en la mayoría de circunstancias.

Para determinar los valores de la escala del impacto que define la materialización de un riesgo o amenaza, se realiza entrevista con el Ingeniero de sistemas preguntándole ¿qué pasaría en un determinado momento, y que tan crítico sería que una de las amenazas identificadas se materialice?, se define una escala donde el valor menos representativo es uno (1); donde se afirma que si el hecho llegará a presentarse tendría consecuencias o efectos mínimos para la empresa, por el contrario si la escala es de cinco (5), tendría desastrosas consecuencias o efectos para la entidad.

IX. PLAN DE TRATAMIENTO DEL RIESGO

Para realizar el tratamiento de los riesgos evaluados se agruparon los activos y sus riesgos por el control que se puede aplicar a varios de ellos, de igual manera, se agruparon por tipo de riesgo con la finalidad de reducir el número de planes a implementar en el área de TI; Todas las políticas que se generen en este plan de tratamiento del riesgo deben ser aprobadas por la alta Gerencia de INDUCON, mediante un acto administrativo. A continuación se enumeran los diferentes planes de tratamiento de los riesgos (véase el Cuadro III)

CUADRO III
IDENTIFICACIÓN DE RIESGOS

No.	Riesgos
1	No disponibilidad del personal (Ausencia accidental del puesto de trabajo: Enfermedad, alteración del orden público.
2	No definición de roles.
3	Persona no capacitada.
4	Uso inadecuado del correo.
5	Descarga de contenido como virus, gusanos y todo clase malware.
6	Administración deficiente de los usuarios con acceso al sistema.
7	Abuso de privilegios.
8	Falta del manual de usuario para el manejo de la aplicación.
9	Daño físico.
10	Daño lógico.
11	Administración deficiente de políticas de contraseña.
12	Mala gestión de directivas de seguridad.
13	Errores de mantenimiento / actualización de software.
14	Principios de privilegios mínimos.
15	Software no licenciado.
16	No existe Backup.

Fuente: Autores

X. LIMITACIONES Y RESTRICCIONES

Para la implementación de un SGSI se requiere realizar las etapas del ciclo PHVA que corresponde a Planificar (plan), Hacer, Verificar y Actuar y un enfoque basado en procesos. La entidad debe establecer una política de seguridad de la información documentada y desplegada a todo el nivel de la organización, definir los perfiles, roles y responsabilidades respecto a la seguridad de la información entre otros.

En la elaboración del plan de seguridad solo se realiza la primera etapa del ciclo del PHVA, estableciendo un diagnóstico del contexto interno y externo de la entidad, se identifican necesidades y expectativas de las partes interesadas sobre seguridad de la información, se clasifican los activos y riesgos y se proponen un plan para el tratamiento de los riesgos con sus acciones, recursos y un cronograma propuesto.

INDUCON, no está lista para un SGSI por que no tiene experiencia en implementación de sistemas de gestión y no cuenta con recursos financieros ni humanos para la implementación, por las anteriores razones se decidió realizar el diseño de un plan de seguridad de la información para el área de TI, con el fin de proponerle a INDUCON acciones concretas para que a mediano plazo implemente un SGSI.

Para continuar con la implementación de un SGSI debe contar con el compromiso de la alta gerencia asignación de recursos y adoptar un enfoque basado en procesos y tomar como punto de partida el diseño del plan de seguridad de la información para el área de TI.

XI. CONCLUSION

Al finalizar el trabajo de investigación aplicada se logran los objetivos planteados, de tal manera que el proyecto propuesto ha contribuido de manera positiva para el interés de INDUCON de mantener la seguridad de sus activos de información respecto a su confidencialidad, integridad y disponibilidad. Así, como identificar al interior del área de TI oportunidades de mejora respecto a la seguridad de la información.

Durante el desarrollo del diseño del plan surgió la necesidad de implementar un control que permitió a la empresa minimizar los riesgos asociados a la descarga de virus, gestionar los accesos al contenido web como son páginas de videos, música y redes sociales, mejorando así el flujo de tráfico en la red, seguridad en las estaciones de trabajo, servidores de aplicación, base de datos y dominio, optimizando el banda ancha y brindando así mejor tráfico para los procesos core de INDUCON.

Finalmente, es importante resaltar que con el diseño del plan no se pretende garantizar la seguridad y protección total de los activos de información, sino llegar a minimizar el riesgo sobre estos a partir de la valoración de los mismos, el reconocimiento de los riesgos las amenazas y vulnerabilidades, logrando la disminución de la probabilidad de ocurrencia, como también de las consecuencias adversas que se generarían de llegar a desencadenarse un incidente de seguridad, es por ello que la formulación y posterior ejecución de medidas de seguridad permitirán a los empleados tener un mejor desempeño respecto al uso de los activos de información, proveyendo de esta manera a la organización herramientas las cuales le permitan hacer de la seguridad de la información no solo un sistema de gestión sino un estilo de vida.

XII. RECOMENDACIONES

Es importante que INDUCON implemente políticas de calidad y un sistema de gestión de calidad, el cual le permitirá organizar e implementar el enfoque basado en procesos en la organización. La documentación de los procesos y el reconocimiento de estos por parte de la organización como documentos organizacionales bajo los cuales se rige un proceso o una determinada actividad, permitirá la mitigación de incidentes de seguridad de la información, ya que existiría un recurso físico bajo el cual los empleados podrían guiar su accionar respecto al proceso que esté vinculado.

Es prioritaria y necesaria la formalización y divulgación de las políticas de seguridad de la información a todo nivel organizacional, con el fin qué esta sea adoptada por todos los funcionarios como una cultura institucional y realizar campañas de socialización y sensibilización de la importancia de la seguridad de la información.

Es importante para INDUCON, la definición y establecimiento de manuales de funciones por competencias. Igualmente que a nivel interno cada área defina roles y responsabilidades a los funcionarios

Se debe exigir a los proveedores de los diferentes sistemas de información los manuales para usuarios finales alineados con los procesos para el uso adecuado de los aplicativos core del negocio.

REFERENCIAS

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001. Bogotá: ICONTEC, 2013. 45 p.

[2] PORTER, Michael E. Modelo de las cinco fuerzas de Porter [en línea]. Bogotá: Wikipedia [citado 18 febrero, 2015]. Disponible en Internet: <URL: es.wikipedia.org/wiki/Análisis_ Porter_de_las_cinco_fuerzas>.

[3] SEGURIDAD EN INFORMACIÓN EN COLOMBIA. Marco legal de Seguridad de la información [en línea]. Bogotá: Blogspot [citado 18 febrero, 2010]. Disponible en Internet: <URL: http://seguridadinformacionColombia.blogspot.com/2010/02/seguir_dad-de-la-informacion-y-seguridad.html>.

[4] EL PORTAL DE ISO 27001 EN ESPAÑOL. ISO 27000 SGSI Sistema de Gestión de Seguridad de la Información [en línea]. Bogotá: El Portal [citado 23 enero, 2015]. Disponible en Internet: <URL: http://www.iso27000.es/sgsi.html>.

[5] TECHNET. Vulnerabilidades de motor de base de datos [en línea]. Madrid: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL:https://technet.microsoft.com/es-es/library/ b895180(v=sql.105).aspx>

[6] Matriz de amenazas y vulnerabilidad motor de base de datos [en línea]. Madrid: La Empresa [citado 18 febrero, 2010]. Disponible en Internet: <URL:https://technet.microsoft.com/es-es/librar/bb895180(v=sql.105).aspx>